Kaspersky Rescue Disk (Notfall-CD)

BENUTZERHANDBUCH

PROGRAMMVERSION: 10.0



Sehr geehrter Benutzer!

Danke, dass Sie sich für unser Produkt entschieden haben. Wir hoffen, dass diese Dokumentation Ihnen hilft und die meisten Fragen damit beantwortet werden können.

Das Dokument kann ohne vorherige Benachrichtigung verändert werden. Die neueste Version finden Sie auf der Seite von Kaspersky Lab unter der Adresse http://www.kaspersky.com/de/docs.

Redaktionsdatum: 30.04.2010

http://www.kaspersky.de
http://support.kaspersky.de

ENDNUTZER-LIZENZVERTRAG

Kaspersky Lab ZAO (der "Rechteinhaber") ist Inhaber aller ausschließlichen Rechte und sonstigen Rechte an der Software.

WICHTIGER RECHTLICHER HINWEIS FÜR ALLE NUTZER: LESEN SIE SICH VOR DER ERSTEN BENUTZUNG DER SOFTWARE ZUNÄCHST DEN FOLGENDEN VERTRAG SORGFÄLTIG DURCH.

INDEM SIE AUF DIE SCHALTFLÄCHE ANNEHMEN IM LIZENZVERTRAG-FENSTER KLICKEN ODER SIE ENTSPRECHENDE ZEICHEN EINGEBEN, ERKLÄREN SIE SICH DAMIT EINVERSTANDEN, DASS DIE BEDINGUNGEN DIESES VERTRAGS VERBINDLICH FÜR SIE SIND. **EINE SOLCHE HANDLUNG IST AUSDRUCK IHRER UNTERSCHRIFT UND SIE SIND DAMIT EINVERSTANDEN, DASS DIESER VERTRAG FÜR SIE VERBINDLICH IST UND SIE VERTRAGSPARTEI SIND. SIE STIMMEN ZU, DASS DIESER VERTRAG GENAUSO DURCHSETZBAR IST WIE JEDER ANDERE VERHANDELTE SCHRIFTLICHE VERTRAG, DEN SIE UNTERZEICHNEN.** WENN SIE NICHT MIT ALLEN BEDINGUNGEN DIESES VERTRAGS EINVERSTANDEN SIND, BRECHEN SIE DIE INSTALLATION DER SOFTWARE BITTE AB UND INSTALLIEREN SIE SIE NICHT.

Der Rechteinhaber gewährt Ihnen hiermit eine einfache, zeitlich unbegrenzte Lizenz für die Speicherung, das Laden, die Installation, Ausführung und Anzeige ("Nutzung") der kostenlosen Software, die im Wesentlichen so funktioniert, wie unter http://support.kaspersky.com/viruses festgelegt ist.

Technischer Support steht nur Nutzern der Produkte Kaspersky Anti-Virus 2011 und Kaspersky Internet Security 2011 zur Verfügung.
Technischer Support: http://support.kaspersky.com

Sie dürfen die Software nicht nachahmen, modifizieren, dekompilieren oder durch Reverse-Engineering bearbeiten oder auf Grundlage der Software oder eines Teils davon abgeleitete Werke zerlegen oder schaffen, wobei die einzige Ausnahme ein unverzichtbares Recht ist, das Ihnen durch geltende Gesetze gewährt wird.

Die Software kann u. U. einige Softwareprogramme beinhalten, die dem Nutzer unter einer GNU General Public License (GPL) (oder Unterlizenz) oder ähnlichen kostenlosen Softwarelizenzen zur Verfügung stehen, die es dem Nutzer, neben anderen Rechten, gestatten, bestimmte Programme oder Teile davon zu kopieren, zu modifizieren und neu zu verteilen und auf den Quellcode zuzugreifen ("Open Source Software"). Wenn gemäß den Lizenzen vorgesehen ist, dass den Nutzern auch der Quellcode für die Software, die in ausführbarem Binärformat weitergegeben wird, zur Verfügung gestellt wird, soll der Quellcode durch Senden einer Anfrage an source@kaspersky.com oder zusammen mit der Software zur Verfügung gestellt werden. Wird im Rahmen von Open Source Software-Lizenzen verlangt, dass der Rechteinhaber Rechte für die Nutzung, das Kopieren oder die Änderung an einem Open Source Softwareprogramm gewährt, die über die in diesem Vertrag gewährten Rechte hinausgehen, dann haben diese Rechte Vorrang vor den hier festgelegten Rechten und Einschränkungen.

DIE SOFTWARE WIRD "OHNE MÄNGELGEWÄHR" BEREITGESTELLT UND DER RECHTEINHABER MACHT KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNGEN BEZÜGLICH IHRER NUTZUNG ODER LEISTUNG AB. MIT AUSNAHME EINER ETWAIGEN GARANTIE, BEDINGUNG, ZUSICHERUNG ODER BESTIMMUNG, DEREN UMFANG NACH GELTENDEN GESETZEN NICHT AUSGESCHLOSSEN ODER EINGESCHRÄNKT WERDEN DARF, GEBEN DER RECHTEINHABER UND SEINE PARTNER KEINE GARANTIE, STELLEN KEINE BEDINGUNG, MACHEN KEINE ZUSICHERUNG ODER BESTIMMUNG (SEI ES EXPLIZIT ODER IMPLIZIT, PER SATZUNG, ALLGEMEINEM RECHT, GEWOHNHEITSRECHT, NUTZUNG ODER ANDERWEITIG) BEZÜGLICH IRGENDEINES ASPEKTS, WOZU OHNE EINSCHRÄNKUNG DIE NICHTVERLETZUNG DER RECHTE DRITTER, VERMARKTUNGSFÄHIGKEIT, ZUFRIEDENSTELLENDE QUALITÄT, INTEGRATION ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK GEHÖREN. SIE ÜBERNEHMEN ALLE MÄNGEL UND DAS GESAMTE RISIKO HINSICHTLICH LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE ZUR UMSETZUNG DER VON IHNEN BEABSICHTIGTEN ZIELE SOWIE FÜR IHRE INSTALLATION, NUTZUNG UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORHERIGEN BESTIMMUNGEN MACHT DER RECHTEINHABER KEINE ZUSICHERUNG UND GIBT KEINE GARANTIE, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON STÖRUNGEN ODER SONSTIGEN MÄNGELN IST ODER DASS DIE SOFTWARE IHRE ANFORDERUNGEN GANZ ODER TEILWEISE ERFÜLLT, UNABHÄNGIG DAVON, OB DIES DEM RECHTEINHABER GEGENÜBER BEKANNT GEMACHT WIRD ODER NICHT.

INHALT

ÜBER DIESES HANDBUCH

Bei diesem Dokument handelt es sich um eine Anleitung zum Booten sowie zur Konfiguration und Verwendung des Programms Kaspersky Rescue Disk. Das Dokument ist für gewöhnliche Anwender gedacht. Zur Verwendung des Programms sind Grundkenntnisse im Umgang mit einem PC erforderlich: Der Anwender sollte das Interface und die Funktionen des Betriebssystems Microsoft Windows auf grundlegendem Niveau beherrschen sowie gängige Programme bedienen können.

Das Dokument soll:

- dem Benutzer dabei helfen, Kaspersky Rescue Disk selbständig zu booten und das Programm unter Berücksichtigung der konkreten Aufgaben des Benutzers optimal zu konfigurieren;
- Fragen, die sich auf das Programm beziehen, schnell beantworten;
- auf alternative Informationsquellen über das Programm und auf Möglichkeiten des technischen Supports hinweisen.

IN DIESEM ABSCHNITT

IN DIESEM DOKUMENT

Das Benutzerhandbuch von Kaspersky Rescue Disk enthält Informationen über das Booten sowie zur Konfiguration und Verwendung von Kaspersky Rescue Disk.

Dieses Dokument enthält folgende Abschnitte:

Zusätzliche Informationsquellen

Dieser Abschnitt enthält Informationen über zusätzliche Informationsquellen zu dem Programm sowie über Internet-Foren, in denen man das Programm diskutieren, Ideen austauschen und Antworten auf seine Fragen erhalten kann.

Kaspersky Rescue Disk

Dieser Abschnitt enthält Informationen über die Neuerungen des Programms sowie eine kurze Beschreibung seiner Grundfunktionen. Außerdem werden die Hard- und Softwarevoraussetzungen genannt, denen ein Computer entsprechen muss, auf dem Kaspersky Rescue Disk funktionieren wird.

Speichern von Kaspersky Rescue Disk auf einem Wechseldatenträger

Dieser Abschnitt enthält eine detaillierte Vorgangsbeschreibung für die Speicherung von Kaspersky Rescue Disk auf einem Wechseldatenträger.

Kaspersky Rescue Disk herunterladen

Dieser Abschnitt enthält Anweisungen, die Ihnen dabei helfen, das Programm auf Ihren Computer zu laden und diesen für die Benutzung von Kaspersky Rescue Disk vorzubereiten.

Arbeit mit Kaspersky Rescue Disk im Grafikmodus

Dieser Abschnitt beschreibt die Arbeit mit Kaspersky Rescue Disk im Grafikmodus. Dieser Abschnitt enthält Informationen über die Oberfläche von Anti-Virus, integrierte Programme und zusätzliche Möglichkeiten von Kaspersky Rescue Disk sowie über das Starten und Beenden Anti-Virus. Dieser Abschnitt enthält Informationen über den Schutzstatus des Computers und darüber, auf welche Weise die Virenuntersuchung von Objekten und die Aktualisierung der Antiviren-Datenbanken auf Ihrem Computer erfolgt. Dieser Abschnitt informiert über die Quarantäne und das Backup, über Berichte und die Arbeit damit. Außerdem bietet der Abschnitt eine Beschreibung der Konfiguration von Kaspersky Rescue Disk.

Arbeit mit Kaspersky Rescue Disk im Textmodus

Dieser Abschnitt beschreibt die Arbeit mit Kaspersky Rescue Disk im Textmodus unter Nutzung des Dateimanagers Midnight Commander. Dieser Abschnitt informiert darüber, auf welche Weise die Virenuntersuchung von Objekten und die Aktualisierung der Antiviren-Datenbanken auf Ihrem Computer erfolgt. Hier finden Sie Informationen zur Netzwerkkonfiguration.

Hardwareinformationen

Dieser Abschnitt beschreibt die Möglichkeit zur Speicherung von Informationen über die Systemhardware in elektronischer Form zur Weitergabe an Kaspersky Lab.

Einschränkungen bei der Programmarbeit

Dieser Abschnitt beschreibt die Beschränkungen in der Arbeit von Kaspersky Rescue Disk.

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt enthält Empfehlungen für die Kontaktaufnahme mit Kaspersky Lab aus Mein Kaspersky Account auf der Seite des Technischen Supports und per Telefon. Außerdem enthält der Abschnitt eine Anleitung zur Erstellung und Speicherung einer Protokolldatei.

Glossar

Dieser Abschnitte enthält eine Liste der Termini, die im Dokument verwendet werden, und deren Definition.

Kaspersky Lab ZAO

Dieser Abschnitt enthält Informationen über den Softwarehersteller Kaspersky Lab. Weiterhin befinden sich dort Beschreibungen anderer Programme und die Kontaktinformationen des Unternehmens.

Information über Fremdcode

Dieser Abschnitt enthält Informationen über Drittcode, der im Programm verwendet wird.

FORMATIERUNG MIT BESONDERER BEDEUTUNG

Die Bedeutung der im Handbuch verwendeten Textformatierungen wird in folgender Tabelle erläutert.

Tabelle 1. Formatierung mit besonderer Bedeutung

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Beachten Sie, dass...	Warnungen sind rot geschrieben und eingerahmt. Die Warnungen enthalten wichtige Informationen, z.B. bezüglich Aktionen, die als kritisch für die Computersicherheit gelten.
Es wird empfohlen,...	Hinweise sind eingerahmt. Hinweise enthalten hilfreiche und informative Angaben.
Beispiel: ...	Beispiele sind gelb unterlegt und mit "Beispiel" überschrieben.
Ein *Update* ist...	Neue Begriffe werden kursiv geschrieben.
ALT+F4	Bezeichnungen von Tasten sind fett und in Großbuchstaben geschrieben. Tastenbezeichnungen, die mit einem Pluszeichen verbunden sind, bedeuten eine Tastenkombination.
Aktivieren	Die Namen von Elementen der Benutzeroberfläche (z.B. Eingabefelder, Menübefehle und Schaltflächen) sind fett geschrieben.
➡ *Gehen Sie folgendermaßen vor, um den Aufgabenzeitplan anzupassen:*	Anweisungen werden durch einen Pfeil gekennzeichnet. Die Einleitungssätze von Anweisungen sind kursiv geschrieben.
`help`	Text in der Befehlszeile oder Meldungstexte, die das Programm auf dem Bildschirm anzeigt, werden durch eine spezielle Schrift hervorgehoben.
<IP-Adresse Ihres Computers>	Variable stehen in eckigen Klammern. Eine Variable wird jeweils durch einen entsprechenden Wert ersetzt, wobei die eckigen Klammern entfallen.

ZUSÄTZLICHE INFORMATIONSQUELLEN

Wenn Sie Fragen zu Auswahl, Kauf, Installation oder Verwendung von Kaspersky Rescue Disk haben, können Sie schnell eine Antwort darauf erhalten.

Kaspersky Lab bietet unterschiedliche Informationsquellen zu dem Programm an. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage unter diesen Quellen wählen.

IN DIESEM ABSCHNITT

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Bei Fragen über die Anwendung stehen folgende Informationsquellen zur Verfügung:

- Seite über das Programm auf der Webseite von Kaspersky Lab.
- Seite über das Programm auf der Webseite des Technischen Supports (in der Wissensdatenbank).
- Elektronisches Hilfesystem.
- Dokumentationen.

Seite auf der Webseite von Kaspersky Lab

Auf der Seite http://support.kaspersky.com/de/viruses/utility finden Sie allgemeine Informationen über Kaspersky Rescue Disk, seine Funktionen und Besonderheiten.

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

Auf der Seite http://support.kaspersky.ru/de/viruses/rescuedisk finden Sie Artikel, die von Support-Experten veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen, die mit der Arbeit von Kaspersky Rescue Disk verbunden.

Elektronisches Hilfesystem

Die Hilfe bietet Informationen darüber, wie der Computerschutz gesteuert wird: Anzeige des Schutzstatus, Untersuchung bestimmter Computerbereiche auf Viren, Ausführen anderer Aufgaben.

Die Hilfe wird durch Klick auf den Link **Hilfe** geöffnet.

Informationen bei Fragen zu einzelnen Fenstern oder Registerkarten von Kaspersky Rescue Disk bietet die Kontexthilfe.

Die Kontexthilfe wird im Fenster des Programms durch Klick auf **Hilfe** oder durch Betätigen der Taste **<F1>** geöffnet.

Dokumentation

Das Benutzerhandbuch von Kaspersky Rescue Disk enthält alle Informationen, die für die Arbeit mit diesem Programm erforderlich sind.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse http://forum.kaspersky.com diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

KONTAKT ZUR ABTEILUNG FÜR DIE HERSTELLUNG VON BENUTZERDOKUMENTATIONEN

Wenn Sie zu dieser Dokumentation Fragen haben, einen Fehler darin entdeckt haben oder Ihre Meinung über unsere Dokumentationen schreiben möchten, richten Sie sich direkt an unsere Abteilung für Handbücher und Hilfesysteme.

Schicken Sie hierzu eine Nachricht mit dem Betreff "Kaspersky Help Feedback: Kaspersky Rescue Disk" an die Mail-Adresse der Abteilung für Handbücher und Hilfesysteme – docfeedback@kaspersky.com.

KASPERSKY RESCUE DISK

Kaspersky Rescue Disk dient zur Untersuchung und Desinfektion infizierter x86- und x64-kompatibler Computer. Das Programm kommt dann zum Einsatz, wenn der Infektionsgrad so hoch ist, dass die Desinfektion eines Computers nicht mehr mit Hilfe von Antiviren-Programmen oder Desinfektionstools (z.B. Kaspersky Virus Removal Tool) möglich ist, die unter dem Betriebssystem gestartet werden. Dabei wird die Effektivität der Desinfektion gesteigert, weil die im System vorhandenen Schädlinge die Kontrolle nicht übernehmen können, während das Betriebssystem hochgefahren wird.

Im Rettungsmodus sind nur die Aufgaben zur Untersuchung von Objekten und zum Update der Datenbanken verfügbar, sowie das Rollback für Updates und die Anzeige der Statistik. Folgende Aktionen können ausgeführt werden:

- Parameter für eine Untersuchungsaufgabe festlegen (siehe Abschnitt "Untersuchungseinstellungen für Objekte" auf S. 45):
  - Sicherheitsstufe ändern (siehe Abschnitt "Ändern der Sicherheitsstufe" auf S. 47);
  - Aktion beim Fund einer Bedrohung ändern (siehe Abschnitt "Ändern der Aktion beim Fund einer Bedrohung" auf S. 48);
  - Liste der Untersuchungsobjekte erstellen (siehe Abschnitt "Liste der Untersuchungsobjekte erstellen" auf S. 30);
  - Typ der zu untersuchenden Objekte ändern (siehe Abschnitt "Ändern des Typs der zu untersuchenden Objekte" auf S. 48);
  - Untersuchungsdauer beschränken (siehe Abschnitt "Beschränkung der Untersuchungsdauer" auf S. 49);
  - Parameter für die Untersuchung zusammengesetzter Dateien festlegen (siehe Abschnitt "Untersuchung von zusammengesetzten Dateien" auf S. 49);
  - Untersuchungsmethode ändern (siehe Abschnitt "Untersuchungsmethode ändern" auf S. 50);
  - Standardmäßige Untersuchungseinstellungen wiederherstellen (siehe Abschnitt "Standardmäßige Untersuchungseinstellungen wiederherstellen" auf S. 51).
- Parameter für die Updateaufgabe festlegen (siehe Abschnitt "Benachrichtigungen deaktivieren" auf S. 60):
  - Updatequelle auswählen (siehe Abschnitt "Auswahl der Updatequelle" auf S. 52);
  - Proxyserver-Parameter anpassen (siehe Abschnitt "Parameter des Proxyservers anpassen" auf S. 53);
  - Regionsoptionen festlegen (siehe Abschnitt "Regionsoptionen der Updatequelle" auf S. 53);
  - Bei Bedarf das letzte Update rückgängig machen (siehe Abschnitt "Rollback zum vorherigen Update" auf S. 32).
- Zusätzliche Einstellungen anpassen (siehe Abschnitt "Erweiterte Programmeinstellungen" auf S. 45):
  - Die Kategorien der erkennbaren Bedrohungen wählen (siehe Abschnitt "Auswahl der Kategorien der erkennbaren Bedrohungen" auf S. 55);
  - Eine vertrauenswürdige Zone anlegen (siehe Abschnitt "Anlegen der vertrauenswürdigen Zone" auf S. 56);
  - Parameter für Benachrichtigungen anpassen (siehe Abschnitt "Einstellungen für Meldungen" auf S. 59);

- Speicherdauer für Berichtsdateien festlegen (siehe Abschnitt "Berichte speichern" auf S. 62);
- Einstellungen für das Speichern von Quarantäne- und Backup-Objekten festlegen (siehe Abschnitt "Quarantäne- und Backup-Objekte speichern" auf S. 63).

- Bericht für Untersuchungs- und Updateaufgaben erstellen (siehe Abschnitt "Berichte" auf S. 36).
- Statistik über die Arbeit des Programms anzeigen (siehe Abschnitt "Berichte" auf S. 36).

IN DIESEM ABSCHNITT

NEUERUNGEN IN KASPERSKY RESCUE DISK

Hier die Neuerungen in Kaspersky Rescue Disk:

- Desinfektion von Autostart-Objekten.
- Heuristische Analyse.
- Aktualisierte Programmmodule.
- Unterstützung von RAID-Massiven.
- Möglichkeit zur Einrichtung eines Netzwerks (einschließlich Wi-Fi).
- Geänderte Funktionsweise des Textmodus.
- Geänderter Bootloader für das Betriebssystem.
- Aktualisierter Betriebssystem-Kernel.
- Aktualisierte Programmpakete von Drittherstellern.
- Neue Programmpakete von Drittherstellern.

HARD- UND SOFTWAREVORAUSSETZUNGEN

Um die normale Funktionsfähigkeit von Kaspersky Rescue Disk zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen:

- *Allgemeine Anforderungen:*
  - CD/DVD-ROM-Laufwerk (für Installation von Kaspersky Rescue Disk von Installations-CD).
  - USB-Port (zur Installation von Kaspersky Rescue Disk von einem bootfähigen Wechseldatenträger).
  - CD-ROM / DVD Writer (für die Speicherung eines Images von Kaspersky Rescue Disk).
  - Unterstützung des Bootens von USB und CD / DVD.
  - Unterstützung der Dateisysteme FAT32/NTFS/Ext2/Ext3/Ext4/Reiser.
  - VESA-kompatible Grafikkarte.
- *Microsoft Windows XP Home Edition (Service Pack 2 oder höher), Microsoft Windows XP Professional (Service Pack 2 oder höher), Microsoft Windows XP Professional x64 Edition (Service Pack 2 oder höher):*
  - Intel Pentium 300 MHz oder höher (oder kompatibel).
  - 256 MB Arbeitsspeicher.
- *Microsoft Windows Vista Home Basic (32/64-Bit), Microsoft Windows Vista Home Premium (32/64-Bit), Microsoft Windows Vista Business (32/64-Bit), Microsoft Windows Vista Enterprise (32/64-Bit), Microsoft Windows Vista Ultimate (32/64-Bit):*
  - Prozessor Intel Pentium 800 MHz 32-Bit (x86)/ 64-Bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor).
  - 512 MB Arbeitsspeicher.
- *Microsoft Windows 7 Starter (32/64 Bit), Microsoft Windows 7 Home Basic (32/64 Bit), Microsoft Windows 7 Home Premium (32/64 Bit), Microsoft Windows 7 Professional (32/64 Bit), Microsoft Windows 7 Ultimate (32/64 Bit):*
  - Prozessor Intel Pentium 1 MHz 32-Bit (x86)/ 64-Bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor).
  - 1 GB Arbeitsspeicher (32-Bit); 2 GB Arbeitsspeicher (64-Bit).

SPEICHERN VON KASPERSKY RESCUE DISK AUF EINEM WECHSELDATENTRÄGER

Dieser Abschnitt enthält eine detaillierte Vorgangsbeschreibung für die Speicherung von Kaspersky Rescue Disk auf einem Wechseldatenträger.

Sie können Kaspersky Rescue Disk mit Hilfe von Kaspersky Anti-Virus 2011 und Kaspersky Internet Security 2011 schnell und bequem erstellen und brennen. Zu diesen Programmen gehört ein spezieller Service, der das Erstellen und Brennen einer Notfall-CD für das System ermöglicht.

IN DIESEM ABSCHNITT

VORBEREITUNG ZUR SPEICHERUNG

Kaspersky Rescue Disk bietet die Möglichkeit der Erstellung eines ISO-Images auf CD / DVD oder auf Wechseldatenträger. Zu Erstellung von Kaspersky Rescue Disk muss der Wechseldatenträger mit dem Dateisystem **Fat16**, **Fat32** oder **NTFS** formatiert und bootfähig gemacht werden.

Selbst bei USB-Datenträgern mit geringer Speicherkapazität nimmt die Formatierung einige Zeit in Anspruch (je größer die Speicherkapazität des Datenträgers, desto länger nimmt die Formatierung in Anspruch). Warten Sie ab, bis die Formatierung abgeschlossen ist.

Um einen Wechseldatenträger bootfähig zu machen, verwenden Sie bitte entsprechende Programme (für Microsoft Windows XP eignet sich z.B. das Programm **Diskpart**, für Microsoft Windows Vista / Microsoft Windows 7 das Programm **HP USB Disk Storage Format Tool**).

SPEICHERN VON KASPERSKY RESCUE DISK

Um ein Image von Kaspersky Rescue Disk auf einem Wechseldatenträger zu speichern, gehen Sie wie folgt vor:

1. Laden Sie das ISO-Image von Kaspersky Rescue Disk vom Kaspersky-Lab-Server herunter.
2. Erstellen Sie auf Ihrem Wechseldatenträger einen Ordner mit dem Namen **rescue**.
3. Kopieren Sie das Image **rescue.iso** auf ihren Wechseldatenträger (<Wechseldatenträger>:\rescue) und benennen Sie es in **rescueusb.iso**.
4. Öffnen Sie das Image **rescueusb.iso** mit Hilfe eines beliebigen ISO-Image-Editors (z.B. **UltraISO**).
5. Kopieren Sie folgende Dateien aus dem Image **rescueusb.iso** auf Ihren Wechseldatenträger (<Wechseldatenträger>:\rescue):
   - README.txt.
   - den Ordner **help**.

6. Kopieren Sie die Datei livecd (vor dem Kopieren umbenennen in liveusb) aus dem Image **rescueusb.iso** auf Ihren Wechseldatenträger (<Wechseldatenträger>:\).

7. Ändern Sie den Inhalt der Datei **boot_from_hard.cfg**, die sich im ISO-Image unter **boot \ grub \ cfg** befindet. Wählen Sie hierzu die Datei aus und klicken Sie in dem mit der rechten Maustaste geöffneten Menü auf **Öffnen mit.** Wählen Sie im folgenden Fenster **Programm aus Liste auswählen**. Klicken Sie auf die Schaltfläche **OK**. Wählen Sie das Programm **Notepad** (**Editor**) aus und klicken Sie auf die Schaltfläche **OK**. Ersetzen Sie die Zeile **root (hd0)** in der geöffneten Datei durch **root (hd1)**. Speichern Sie die Änderungen.

> Ändern Sie den Inhalt der Datei **boot_from_hard.cfg**, wenn Sie mit dem auf den Wechseldatenträger geschriebenen Programm Kaspersky Rescue Disk arbeiten. Dies ist für das korrekte Laden des Betriebssystems von der Festplatte erforderlich.
>
> In einigen Konfigurationen der Hard- bzw. Software ist das Booten von Festplatte unmöglich. Entfernen Sie in diesem Fall Ihren Wechseldatenträger, starten Sie den Computer neu, und überprüfen Sie, dass das Bootgerät im BIOS die Festplatte mit dem Betriebssystem ist.

8. Entfernen sie alles aus dem ISO-Image **rescueusb.iso** außer dem Ordner **boot**. Speichern Sie die Änderungen.

9. Kopieren Sie das Original-Image **rescue.iso** auf <Wechseldatenträger>:\rescue. Jetzt befinden sich auf dem Wechseldatenträger zwei ISO-Images: **rescueusb.iso** und **rescue.iso**.

> **Rescueusb.iso** ist nur für das Laden von grub2 und das anfängliche Booten von Linux erforderlich.

10. Laden Sie das Archiv unter dem Link http://nufans.net/grub4dos/grub4dos-0.4,4-2009-10-16.zip herunter. Entpacken Sie es in einen gleichnamigen Ordner. Öffnen Sie den entpackten Ordner.

11. Kopieren sie folgende Dateien aus dem vorgenannten Ordner in das Wurzelverzeichnis Ihres Wechseldatenträgers:

    - grldr.
    - menu.lst.

    Ändern Sie den Inhalt der Datei **menu.lst**. Wählen Sie hierzu die Datei aus und klicken Sie in dem mit der rechten Maustaste geöffneten Menü auf **Öffnen mit.** Wählen Sie im folgenden Fenster **Programm aus Liste auswählen**. Klicken Sie auf die Schaltfläche **OK**. Wählen Sie das Programm **Notepad** (**Editor**) aus und klicken Sie auf die Schaltfläche **OK**. Entfernen Sie den gesamten Inhalt der Datei und ersetzen sie ihn unter genauer Einhaltung der Syntax durch den folgenden Ausdruck:

```
map (hd0,0)/rescue/rescueusb.iso (0xff) || map --mem
(hd0,0)/rescue/rescueusb.iso (0xff)

map --hook

chainloader (0xff)
```

    Speichern Sie die Änderungen.

12. Prüfen Sie den Laufwerksbuchstaben, der Ihrem Wechseldatenträger zugeordnet wurde.

    Wählen Sie dazu in der Taskleiste Ihres Betriebssystems den Menüpunkt **Start** → **Systemsteuerung** → **Verwaltung** → **Computerverwaltung** aus. Wählen Sie im erscheinenden Fenster aus der Liste das Element **Datenträgerverwaltung** aus. Im rechten Teil des Fensters öffnet sich eine Liste der verbundenen Laufwerke. Wählen Sie Ihren Wechseldatenträger aus und merken Sie sich seinen Buchstaben.

13. Laden Sie das Archiv unter dem Link http://download.gna.org/grubutil/grubinst-1,1-bin-w32-2008-01-01.zip.

14. Öffnen Sie die Befehlszeile. Wählen Sie hierzu in der Taskleiste Ihres Betriebssystems den Menüpunkt **Start** → **Ausführen** aus und geben Sie im Feld **Öffnen cmd** ein.

15. Geben Sie in der Befehlszeile **"Pfad des geladenen Archivs\grubinst.exe" (hdN)** ein, wobei **N** für den Buchstaben Ihres Laufwerks steht.

KASPERSKY RESCUE DISK HERUNTERLADEN

Dieser Abschnitt enthält Anweisungen, die Ihnen dabei helfen, das Programm auf Ihren Computer zu laden und diesen für die Benutzung von Kaspersky Rescue Disk vorzubereiten.

IN DIESEM ABSCHNITT

VORBEREITUNG ZUM HERUNTERLADEN

Bevor Kaspersky Rescue Disk heruntergeladen wird, gehen Sie folgendermaßen vor:

1. Wählen Sie in den BIOS-Einstellungen das Booten von CD/DVD-ROM oder von einem Wechseldatenträger (weitere Informationen finden Sie in der Dokumentation zum Motherboard Ihres Computers).

2. Legen Sie eine CD/DVD-ROM mit einem Image von Kaspersky Rescue Disk ein oder schließen Sie einen Wechseldatenträger damit an der USB-Schnittstelle des Computers an.

3. Starten Sie den Computer neu. Nach dem Neustart erscheint die Meldung **Press any key to enter the menu** auf dem Bildschirm.

4. Drücken Sie eine beliebige Taste. Der Bootmanager wird gestartet.

   Wird innerhalb von zehn Sekunden keine Taste betätigt, bootet der Computer automatisch von der Festplatte.

HERUNTERLADEN VON KASPERSKY RESCUE DISK

Gehen Sie folgendermaßen vor, um das Booten von Kaspersky Rescue Disk fortzusetzen:

1. Wählen Sie in dem sich öffnenden Bootmanager mit Hilfe der Cursortasten die Sprache der Grafikoberfläche aus. Klicken Sie auf die Taste **ENTER**.

   Es erscheint ein Fenster mit den zur Verfügung stehenden Optionen.

2. Wählen Sie einen der folgenden Bootoptionen aus:

   - **Betriebssystem starten**.

     In einigen Konfigurationen der Hard- bzw. Software ist das Booten von Festplatte unmöglich. Entfernen Sie in diesem Fall Ihren Wechseldatenträger, starten Sie den Computer neu, und überprüfen Sie, dass das Bootgerät im BIOS die Festplatte mit dem Betriebssystem ist.

   - Kaspersky Rescue Disk. **Grafikmodus** bootet das Grafik-Subsystem.

- Kaspersky Rescue Disk. **Textmodus** bootet die Textoberfläche in Form des Konsolen-Dateimanagers **Midnight Commander (MC)**.

Außerdem können Sie Informationen über die Hardware Ihres Computers ermitteln und speichern (s. Abschnitt "Hardwareinformationen" auf S. 72), den Computer von der Festplatte booten und den Computer neu starten oder herunterfahren. Verwenden Sie dazu die entsprechenden Punkte der Liste.

Klicken Sie auf die Taste **ENTER**.

Hierauf wird das Betriebssystem Linux mit Ermittlung der Geräte gebootet und eine Suche der Dateisysteme auf internen und externen Laufwerken durchgeführt. Gefundene Dateisysteme und externe Geräte erhalten Namen, die vom installierten Betriebssystem verwendet werden.

Befindet sich das Betriebssystem des zu bootenden Computers im Standby-Modus oder wurde es nicht ordnungsgemäß heruntergefahren, wird Ihnen vorgeschlagen, das Dateisystem zu mounten oder den Computer neu zu starten. In diesem Fall muss eine von drei Varianten ausgewählt werden:

- **Fortsetzen**. Das Programm fährt mit dem Mounten des Dateisystems fort, wobei es jedoch zu einer Beschädigung des Dateisystems kommen kann.
- **Überspringen**. Das Programm überspringt das Mounten des Dateisystems. In diesem Fall können Sie nur die Bootsektoren und die Autostart-Elemente auf Viren untersuchen.

  Einige Dateisysteme können gemountet werden.

- **Computer neu starten**. Diese Option ermöglicht Ihnen ein Booten von der Festplatte, um das Betriebssystem ordnungsgemäß herunterzufahren.

Der weitere Bootprozess erfolgt in folgender Reihenfolge:

a. Die Auslagerungsdatei von Microsoft Windows pagefile.sys wird gesucht. Wenn sie nicht vorhanden ist, wird die Größe des virtuellen Speichers durch die Größe des Arbeitsspeichers begrenzt.

b. Es werden Ordner zum Speichern von Antiviren-Datenbanken, Berichten, Quarantäne und sonstigen Dateien erstellt.

c. Konfiguration der Netzwerkverbindungen auf Grundlage der Daten, die in den Systemdateien des hochgefahrenen Computers gefunden werden.

d. Start von Anti-Virus, wenn der Grafikmodus ausgewählt wurde. Start des Dateimanagers **Midnight Commander** mit geöffnetem Benutzermenü, wenn der Textmodus ausgewählt wurde.

ARBEIT MIT KASPERSKY RESCUE DISK IM GRAFIKMODUS

Dieser Abschnitt beschreibt die Arbeit mit Kaspersky Rescue Disk im Grafikmodus.

IN DIESEM ABSCHNITT

OBERFLÄCHE VON KASPERSKY RESCUE DISK

Dieser Abschnitt enthält Informationen über das Interface von Anti-Virus, integrierte Programme und zusätzliche Möglichkeiten von Kaspersky Rescue Disk.

IN DIESEM ABSCHNITT

TASKLEISTE

Bei der Taskleiste handelt es sich um eine Leiste im unteren Teil des Bildschirms, auf der sich das Symbol befindet. Durch Klicken auf das Symbol können Sie das Menü von Kaspersky Rescue Disk öffnen. Sie können das Menü auch über die rechte Maustaste öffnen, wenn Sie den Cursor an einer freien Stelle des Desktops platzieren.

Es öffnet sich dann ein Menü, das einen bequemen Zugriff auf die Systemelemente gewährleistet (s. Abb. unten).



Abbildung 1. Menü von Kaspersky Rescue Disk

Das Menü enthält Punkte, bei deren Auswahl folgende Instrumente zur Verfügung stehen:

- **Kaspersky Rescue Disk** – startet Anti-Virus.
- **Dateimanager** (auf S. 24) – startet den Dateimanager **X File Explorer (xfe)**.
- **Webbrowser** (auf S. 25) – startet den Webbrowser **Mozilla Firefox**.
- **Terminal** (auf S. 25) – startet die Betriebssystemkonsole.
- **Screenshot erstellen** (auf S. 25) – kopiert den gesamten Bildschirm, wie er auf dem Monitor angezeigt wird, und zeigt den Pfad zur gespeicherten Datei an.
- **Netzwerk konfigurieren** (auf S. 25) – öffnet das Fenster für die Netzwerkkonfiguration. Im erscheinenden Fenster ist die Konfiguration des Netzwerkadapters und die Änderung der Proxyserver-Parameter möglich.
- **Über Kaspersky Rescue Disk** – öffnet ein Fenster mit Informationen zur Version von Kaspersky Rescue Disk.
- **Computer neu starten** – öffnet ein Fenster, in dem der Neustart des Computers bestätigt werden muss.
- **Computer ausschalten** – öffnet ein Fenster, in dem die Beendigung der Arbeit mit dem Computer bestätigt werden muss.

Außerdem können Sie die Anordnung aller offenen Fenster auf dem Desktop ändern. Öffnen Sie hierzu an einer freien Stelle der Taskleiste das Kontextmenü durch Betätigung der rechten Maustaste und wählen Sie die erforderliche Aktion aus.

OBERFLÄCHE VON ANTI-VIRUS

In diesem Abschnitt werden die wichtigsten Elemente der Anti-Virus-Oberfläche behandelt.

IN DIESEM ABSCHNITT

PROGRAMMHAUPTFENSTER

Das Hauptfenster von Kaspersky Rescue Disk ist für die Nutzung aller Möglichkeiten des Programms vorgesehen.

Das Programmhauptfenster lässt sich bedingt in zwei Bereiche aufteilen:

- Der obere Bereich des Fensters informiert über den aktuellen Schutzstatus Ihres Computers.

  Es gibt drei Varianten für den Schutzstatus (siehe Abschnitt "Schutzstatus des Computers" auf S. 26). Jeder Status wird durch eine Farbe signalisiert. Die Farben entsprechen den Signalen einer Ampel. Die Farbe Grün bedeutet, dass der Schutz Ihres Computers dem erforderlichen Niveau entspricht. Gelb und Rot signalisieren, dass bestimmte Sicherheitsbedrohungen vorliegen. Als Bedrohung gilt nicht nur der Fund schädlicher Programme, sondern auch die Verwendung veralteter Datenbanken, die Auswahl einer niedrigen Sicherheitsstufe u.a.

  Vorhandene Sicherheitsrisiken sollten umgehend behoben werden. Um ausführliche Informationen darüber zu erhalten und die Bedrohungen schnell zu beheben, klicken Sie auf das Symbol für den Status (s. Abb. oben).

- Der zentrale Teil des Fensters ermöglicht durch Auswahl der entsprechenden Registerkarte den Wechsel zur Ausführung der Aufgabe zur Untersuchung von Objekten oder der Update-Aufgabe:

- Auf der Registerkarte **Untersuchung von Objekten** (s. Abb. unten), können Sie folgende Aktionen ausführen:
  - Starten / Beenden der Aufgabe zur Untersuchung von Objekten (siehe Abschnitt "Starten und Beenden der Aufgabe zur Untersuchung von Objekten" auf S. 30);
  - einzelnen Laufwerke, Verzeichnisse oder Dateien des Computers zu der Untersuchungsaufgabe hinzuzufügen oder aus dieser entfernen (siehe Abschnitt "Liste der Untersuchungsobjekte erstellen" auf S. 30);
  - Anzeigen des Fortschritts und des Ergebnisses der Untersuchungsaufgabe.

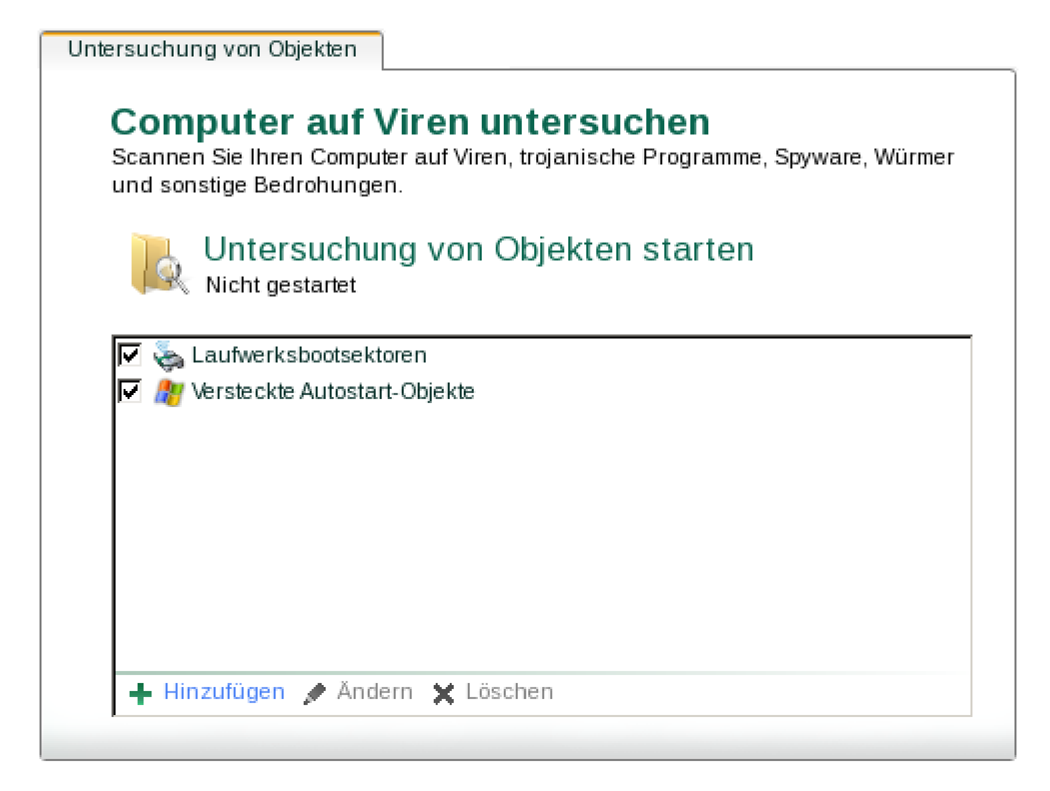


Abbildung 2. Registerkarte "Untersuchung von Objekten"

- Auf der Registerkarte **Update** (s. Abb. unten), können Sie folgende Aktionen ausführen:
  - Starten / Beenden der Update-Aufgabe (siehe Abschnitt "Start und Beenden der Updateaufgabe" auf S. 32);
  - Anzeigen einer Übersicht über die Virenaktivität durch Betätigen des gleichnamigen Links;
  - Rollback der Datenbanken zur vorherigen Version (siehe Abschnitt "Rollback zum vorherigen Update" auf S. 32);
  - Anzeigen des Fortschritts und des Ergebnisses der Update-Aufgabe.

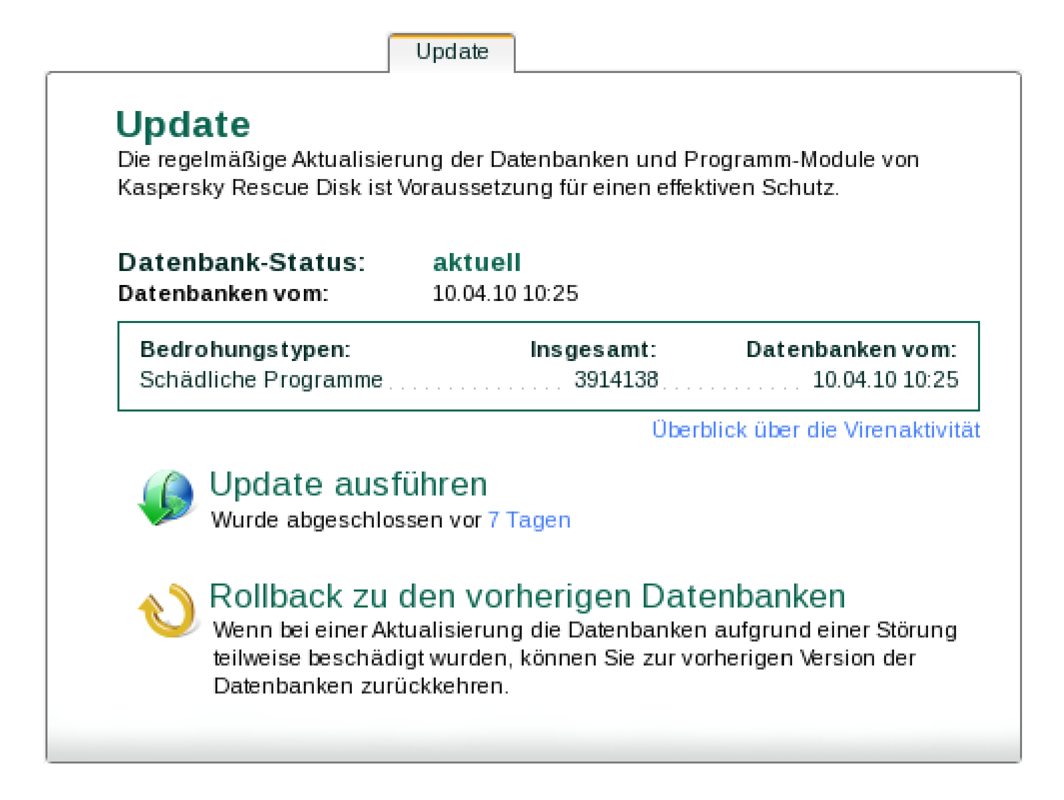


Abbildung 3. Registerkarte "Update"

Außerdem stehen folgende Schaltflächen und Links zur Verfügung:

- **Einstellungen** – in das Programmkonfigurationsfenster wechseln.
- **Quarantäne** – zur Arbeit mit Objekten, die in die Quarantäne verschoben wurden, wechseln.
- **Bericht** – zu einer Liste der Ereignisse, die bei der Arbeit des Programms eingetreten sind, wechseln.
- **Hilfe** – zum Hilfesystem für Kaspersky Rescue Disk wechseln.
- **Beenden** – beendet Anti-Virus.

KONFIGURATIONSFENSTER

Das Konfigurationsfenster von Kaspersky Rescue Disk lässt sich über den Link **Einstellungen** im oberen Teil des Hauptfensters öffnen. Dieses Fenster unterstützt Sie bei der Konfiguration von Kaspersky Rescue Disk.

Das Konfigurationsfenster besteht aus zwei Teilen:

- Der linke Teil des Fensters gewährt Zugriff auf die Aufgabe zur Untersuchung von Objekten und zum Update sowie zur Einstellung der Parameter für Bedrohungen und Ausnahmen, Benachrichtigungen, Berichten und Speichern von Kaspersky Rescue Disk;
- Der rechte Teil des Fensters enthält eine Liste einstellbaren Parameter für den im linken Teil des Fensters ausgewählten Bereich.

MELDUNGEN

Wenn bei der Arbeit von Kaspersky Rescue Disk bestimmte Ereignisse eintreten, werden Sie durch Popupmeldungen darüber informiert.

In Abhängigkeit davon, welche Relevanz das Ereignis für die Computersicherheit besitzt, sind folgende Arten von Meldungen möglich:

- **Alarm**. Ein Ereignis mit kritischer Priorität ist eingetreten. Beispiel: ein Virus wurde gefunden. Die sofortige Entscheidung über das weitere Vorgehen ist erforderlich. Meldungen dieses Typs besitzen rote Farbe.
- **Achtung**. Ein potentiell gefährliches Ereignis ist eingetreten. Beispiel, ein möglicherweise infiziertes Objekt wurde gefunden. Sie werden aufgefordert, über die Gefährlichkeit dieses Ereignisses zu entscheiden. Meldungen dieses Typs besitzen gelbe Farbe.
- **Informationen**. Diese Meldung informiert über ein Ereignis, das keine vorrangige Priorität besitzt. Informative Meldungen dieses Typs besitzen grüne Farbe.

ZUSÄTZLICHE TOOLS

In diesem Abschnitt werden die Programme beschrieben, die zu Kaspersky Rescue Disk gehören, und die von Kaspersky Rescue Disk bereitgestellten zusätzlichen Möglichkeiten.

IN DIESEM ABSCHNITT

DATEIMANAGER

Der integrierte Dateimanager **X File Explorer (xfe)** basiert auf dem beliebten Projekt X Win Commander, das heute allerdings nicht mehr weiterentwickelt wird. **X File Explorer** verfügt über eine intuitiv verständliche Benutzeroberfläche und ist ein für Anfänger und erfahrene Benutzer gleichermaßen nützliches Werkzeug für die Arbeit mit Dateien.

Homepage des Projekts: http://roland65.free.fr/xfe/

WEBBROWSER

Mit dem Internet-Browser Firefox, der zum Lieferumfang von Kaspersky Rescue Disk gehört, lassen sich Webseiten anzeigen und aufgerufene Seiten speichern. Die gespeicherten Seiten lassen sich auch nach dem Beenden der Arbeit mit Kaspersky Rescue Disk ansehen.

Für das Aufrufen von Webseiten mit dem integrierten Browser ist ein Internetzugang über ein lokales Netzwerk erforderlich (Local Area Network connection). Der Webbrowser arbeitet standardmäßig mit dem Proxyserver des Systems. Sie können spezielle Proxyserver-Einstellungen für den Webbrowser festlegen. Standardmäßig ist die offizielle Homepage von Kaspersky Lab als Startseite des Browsers eingerichtet.

TERMINAL

Das Terminal ist eine Betriebssystemkonsole, die für die Arbeit mit der Befehlszeile im Grafikmodus vorgesehen ist.

SCREENSHOT

Diese Option ermöglicht es, den Bildschirm so zu kopieren, wie er auf dem Monitor angezeigt wird, und sich den Pfad zur gespeicherten Datei anzusehen.

NETZWERK KONFIGURIEREN

Diese Option erlaubt es, den Netzwerkadapter anzupassen und die Einstellungen des systemeigenen Proxyservers zu ändern. Nach einer Änderung der Proxyserver-Einstellungen, arbeiten die Updateaufgabe und der Browser mit den neuen Einstellungen.

Für die Updateaufgabe (siehe Abschnitt "Parameter des Proxyservers anpassen" auf S. 53) und für den Browser (siehe Abschnitt "Webbrowser" auf S. 25) können auch individuelle Proxyserver-Einstellungen festgelegt werden.

STARTEN UND BEENDEN VON ANTI-VIRUS

Dieser Abschnitt enthält Informationen über das Starten und Beenden von Anti-Virus.

IN DIESEM ABSCHNITT

START VON ANTI-VIRUS

➡ *Führen Sie zum Start von Anti-Virus eine der folgenden Aktionen aus:*

- Rufen Sie an einer freien Stelle des Desktops durch Klicken der rechten Maustaste das Kontextmenü auf und wählen Sie den Punkt **Kaspersky Rescue Disk**.
- Klicken Sie auf das Symbol in der Taskleiste. Wählen Sie im erscheinenden Menü den Punkt **Kaspersky Rescue Disk** aus.

Anti-Virus startet direkt nach dem Booten von Kaspersky Rescue Disk im Grafikmodus automatisch.

BEENDEN VON ANTI-VIRUS

➡ *Um die Arbeit von Anti-Virus zu beenden, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf die Schaltfläche **Beenden**.

   Auf dem Bildschirm erscheint ein Dialogfenster mit der Frage **Wollen Sie Kaspersky Rescue Disk wirklich beenden?**

2. Klicken Sie auf die Schaltfläche **Ja**.

SCHUTZSTATUS DES COMPUTERS

Über das Auftreten von Problemen im Computerschutz informiert der Schutzstatus des Computers. Die Farbe des Schutzsymbols wird verändert (s. Abb. unten).



Abbildung 4. Aktueller Schutzstatus des Computers

Es gibt drei Varianten für den Schutzstatus. Jeder Status wird durch eine Farbe signalisiert. Die Farben entsprechen den Signalen einer Ampel.

- Grün. Diese Farbe weist darauf hin, dass der Schutz des Computers dem erforderlichen Niveau entspricht. - Die Datenbanken für Kaspersky Rescue Disk wurden rechtzeitig aktualisiert, und bei der Untersuchung des Computers wurden keine schädlichen Objekte gefunden oder alle gefundenen Objekte wurden neutralisiert.



- Gelb. Diese Farbe signalisiert ein verringertes Schutzniveau. Beispiel: Die Datenbanken sind veraltet.

- Rot. Diese Farbe signalisiert die Existenz von Problemen, die zur Infektion des Computers und zu Datenverlust führen können: z.B. das Programm wurde sehr lange nicht mehr aktualisiert oder es wurden schädliche Objekte gefunden, die dringend neutralisiert werden müssen.

Die Bedrohungen sind jeweils bei ihrem Auftreten zu beseitigen. Durch Klick auf das Symbol des Status (s. Abb. oben), gelangen Sie auf die Registerkarte **Status** (s. Abb. unten), die eine Liste der aufgetretenen Probleme enthält und entsprechende Lösungsmöglichkeiten bietet.

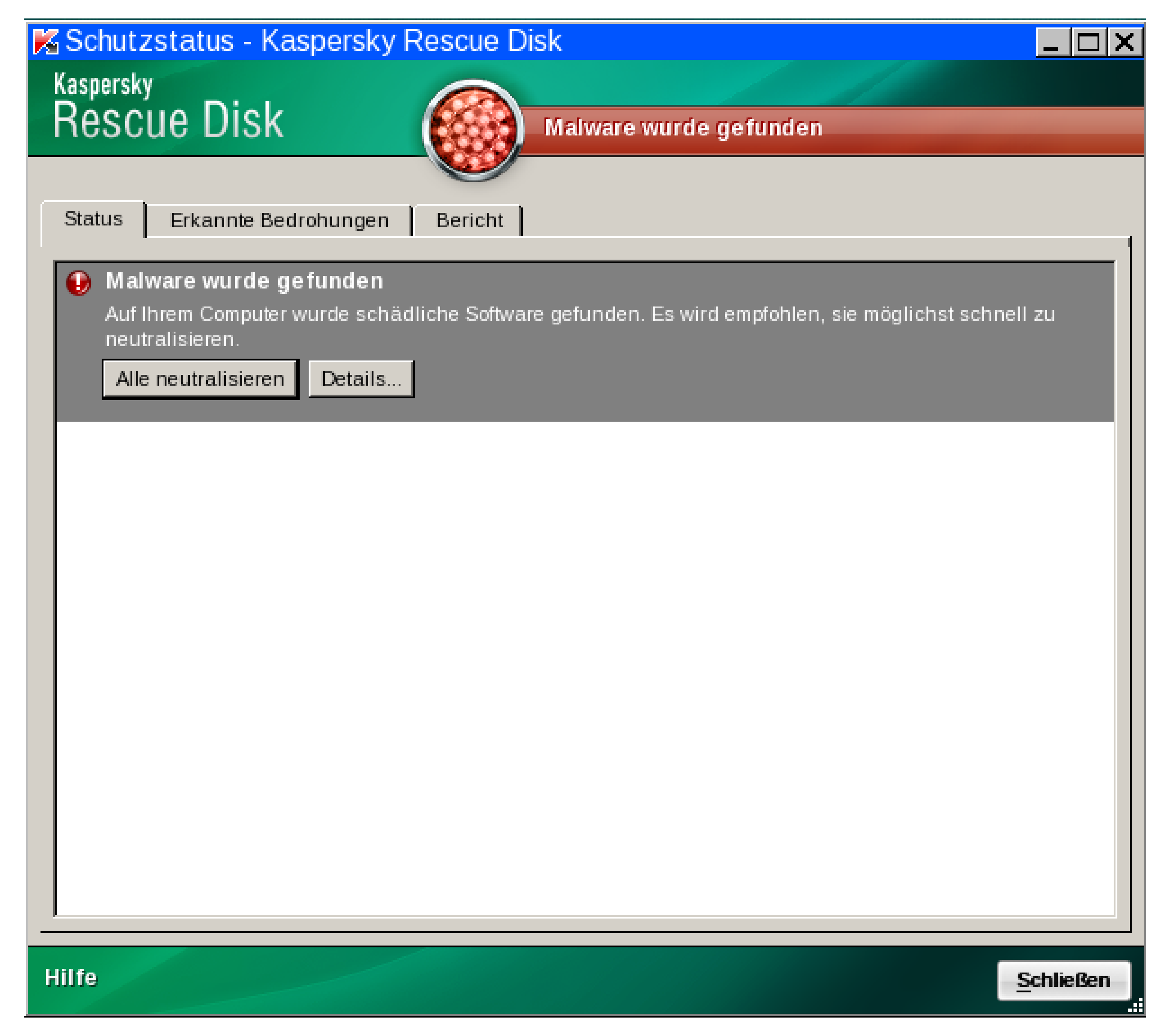


Abbildung 5. Sicherheitsprobleme beheben

Die Probleme sind ihrer Priorität entsprechend angeordnet und sollten in dieser Reihenfolge gelöst werden: Zu Beginn stehen die wichtigsten Probleme, die mit einem rotem Symbol gekennzeichnet sind, danach die weniger wichtigen mit gelbem Symbol und zum Schluss informative Meldungen mit grünem Symbol. Für jedes Problem ist eine ausführliche Beschreibung vorhanden.

Für das Problem **Malware wurde gefunden** werden folgende Aktionen angeboten:

- **Alle neutralisieren**. Durch Klicken auf die Schaltfläche **Alle neutralisieren**, können Sie zur sofortigen Neutralisierung der Probleme übergehen, was der empfohlenen Aktion entspricht.
- **Details**. Durch Klicken auf die Schaltfläche **Details** gelangen Sie auf die Registerkarte **Erkannte Bedrohungen**, wo Sie ausführliche Informationen über eine gefundene Bedrohung anzeigen können.

Für das Problem **Die Datenbanken sind veraltet** werden folgende Aktionen angeboten:

- **Jetzt aktualisieren**. Durch Klicken auf die Schaltfläche **Jetzt aktualisieren**, gelangen Sie auf der Registerkarte **Update**, von dem die Updateaufgabe gestartet werden kann.

Um Meldungen wieder anzuzeigen, die zuvor ausgeblendet wurden, klicken Sie im Block **Einige Meldungen wurden ausgeblendet** auf die Schaltfläche **Ausgeblendete Meldungen anzeigen**.

UNTERSUCHUNG VON OBJEKTEN

Dieser Abschnitt enthält Informationen darüber, auf welche Weise die Untersuchung von Objekten auf Ihrem Computer durch Kaspersky Rescue Disk erfolgt.

IN DIESEM ABSCHNITT

VIRENSUCHE

Die Virensuche ist eine der wichtigsten Funktionen für die Sicherheit des Computers. Durch die Virensuche lässt sich die Ausbreitung von schädlichem Code erkennen, der aus bestimmten Gründen nicht vom Malware-Schutz erkannt wurde.

Nach dem Start der Aufgabe zur Untersuchung von Objekten (siehe Abschnitt "Starten und Beenden der Aufgabe zur Untersuchung von Objekten" auf S. 30) untersucht Kaspersky Rescue Disk die vom Benutzer festlegten Objekte. Jedes Objekt des Computer-Dateisystems kann untersucht werden.

Standardmäßig entspricht jeder Aufgabe zur Untersuchung von Objekten eine Liste von Objekten. Zu diesen Objekten gehören Bootsektoren und Dateien auf logischen Laufwerken. Sie können diese Liste ändern (siehe Abschnitt "Liste der Untersuchungsobjekte erstellen" auf S. 30).

Logische Datenträger, denen im Betriebssystem Windows kein Laufwerksname zugewiesen wurde, werden als sdbN angezeigt. Dabei steht N für die Nummer, die dem Datenträger von dem Programm Kaspersky Rescue Disk zugewiesen wurde (s. Abb. unten).



Abbildung 6. Logische Datenträger, denen im Betriebssystem Windows kein Laufwerksname zugewiesen wurde

Der Aufgabe zur Virensuche entspricht eine bestimmte Auswahl von Parametern, die auf der Oberfläche von Kaspersky Rescue Disk standardmäßig eingestellt ist. Diese Parameter gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst. Wenn die vordefinierte Stufe Ihren Anforderungen nicht entspricht, können Sie folgende Aktionen ausführen:

- Sicherheitsstufe ändern (siehe Abschnitt "Ändern der Sicherheitsstufe" auf S. 47);
- Dateitypen, die auf Viren untersucht werden sollen, festlegen (siehe Abschnitt "Ändern des Typs der zu untersuchenden Objekte" auf S. 48);
- Untersuchungsdauer beschränken (siehe Abschnitt "Beschränkung der Untersuchungsdauer" auf S. 49);
- Parameter für die Untersuchung zusammengesetzter Dateien anpassen (siehe Abschnitt "Untersuchung von zusammengesetzten Dateien" auf S. 49);
- Untersuchungsmethode wählen (siehe Abschnitt "Untersuchungsmethode ändern" auf S. 50), die die Ausführlichkeit der Untersuchung beeinflusst;
- Aktion beim Fund einer Bedrohung festlegen (siehe Abschnitt "Ändern der Aktion beim Fund einer Bedrohung" auf S. 48).

Während Sie die Einstellungen einer Untersuchungsaufgabe anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren (siehe Abschnitt "Standardmäßige Untersuchungseinstellungen wiederherstellen" auf S. 51).

Informationen über den Verlauf der Aufgabenausführung werden im Hauptfenster von Kaspersky Rescue Disk auf der Registerkarte **Untersuchung von Objekten** im Feld unter dem Namen der gestarteten Aufgabe angezeigt.

Die Ergebnisse einer Virensuche werden im Bericht von Kaspersky Rescue Disk aufgezeichnet (der Link **Bericht** im oberen Bereich des Fensters).

SIEHE AUCH

STARTEN UND BEENDEN DER AUFGABE ZUR UNTERSUCHUNG VON OBJEKTEN

Gehen Sie folgendermaßen vor, um eine Aufgabe zur Untersuchung von Objekten zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf der Registerkarte **Untersuchung von Objekten** auf **Untersuchung von Objekten starten**. Klicken Sie auf **Untersuchung von Objekten abbrechen** falls eine laufende Aufgabe beendet werden soll.

   Der Fortschritt und das Ergebnis der Ausführung der Untersuchungsaufgabe werden im folgenden Fenster dargestellt.

SIEHE AUCH

LISTE DER UNTERSUCHUNGSOBJEKTE ERSTELLEN

Gehen Sie folgendermaßen vor, um eine Liste der Untersuchungsobjekte zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Auf der Registerkarte **Untersuchung von Objekten**, gehen Sie folgendermaßen vor:

   - Gelangen Sie über den Link **Hinzufügen**. Das Fenster **Untersuchungsobjekt auswählen** wird geöffnet. Fügen Sie das Objekt zur Liste der Untersuchungsobjekte hinzu.

     Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie auf **OK**.

     Wenn beim Hinzufügen eines Objekts das Kontrollkästchen ☑ **Unterordner einschließen** aktiviert wurde, erfolgt eine rekursive Untersuchung.

   - Verwenden Sie den Link **Löschen**, um ein Objekt aus der Liste zu löschen.
   - Ändern Sie das Objekt aus der Liste durch Klick auf den Link **Ändern**.

   Objekte können auch vorübergehend von der Untersuchung ausgeschlossen werden, ohne aus der Liste gelöscht zu werden. Markieren Sie dazu das Objekt in der Liste und deaktivieren Sie das entsprechende Kontrollkästchen.

Objekte, die sich standardmäßig in der Liste befinden, können nicht geändert oder gelöscht werden.

Wenn der Untersuchungsbereich leer ist oder kein Objekt des Untersuchungsbereichs angekreuzt wurde, kann die Aufgabe zum Scan auf Befehl nicht gestartet werden!

SIEHE AUCH

Update

Dieser Abschnitt enthält Informationen darüber, auf welche Weise die Aktualisierung der Antiviren-Datenbanken auf Ihrem Computer durch Kaspersky Rescue Disk erfolgt.

In diesem Abschnitt

Update

Eine Voraussetzung für die Sicherheit Ihres Computers besteht darin, den Schutz auf dem neusten Stand zu halten. Jeden Tag tauchen neue Viren, trojanische und andere schädliche Programme auf. Und es ist sehr wichtig sicherzustellen, dass Ihre Informationen zuverlässig geschützt werden. Informationen über Bedrohungssignaturen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Rescue Disk enthalten. Deshalb stellt die regelmäßige Aktualisierung der Datenbanken einen sehr wichtigen Sicherheitsfaktor dar.

Für die Aktualisierung der Antiviren-Datenbanken muss die Updateaufgabe gestartet werden (siehe Abschnitt "Start und Beenden der Updateaufgabe" auf S. 32). Dabei lädt Kaspersky Rescue Disk die Updates auf Ihren Computer herunter und installiert sie.

Wenn Sie die Datenbanken aktualisiert haben und diese bei der Arbeit beschädigt wurden, können Sie Update rückgängig machen (s. Abschnitt "Rollback zum vorherigen Update" auf S. 32). Bevor die Datenbanken aktualisiert werden, legt Kaspersky Rescue Disk eine Sicherungskopie davon an. Bei Bedarf können Sie zur vorhergehenden Version der Datenbanken zurückkehren.

Das Update von Kaspersky Rescue Disk wird anhand einer bestimmten Auswahl von standardmäßigen Parametern ausgeführt.

Wenn keine der vordefinierten Parametern Ihren Anforderungen entsprechen, können Sie folgende Aktionen ausführen:

- eine andere Updatequelle auswählen (siehe Abschnitt "Auswahl der Updatequelle" auf S. 52);
- Regionsoptionen der Updatequelle ändern (siehe Abschnitt "Regionsoptionen der Updatequelle" auf S. 53);
- Proxyserver-Parameter festlegen (siehe Abschnitt "Parameter des Proxyservers anpassen" auf S. 53).

Die Antiviren-Datenbanken müssen ständig aktualisiert werden. Über die Notwendigkeit einer Aktualisierung können Sie sich auf der Registerkarte **Update** im Programmhauptfenster informieren. Auf der Registerkarte werden die folgenden Parameter angezeigt:

- Status der Datenbanken (aktuell, veraltet oder beschädigt).

  Bei Auswahl der Updatequelle (siehe Abschnitt "Updatequelle auswählen" auf S. 52) werden die Antiviren-Datenbanken auf Ihrem Computer mit den auf der Updatequelle vorhandenen verglichen. Wenn Datenbanken nicht aktuell sind, wird nur der fehlende Teil der Updates auf Ihrem Computer installiert.

- Datum und Uhrzeit des Erscheinens.
- Anzahl und Zusammensetzung der Einträge in den Datenbanken.

Sie können zum Bericht über das Update wechseln, der vollständige Informationen über die Ereignisse, die bei der Ausführung der Updateaufgabe eingetreten sind, bietet (der Link **Bericht** im oberen Bereich des Fensters). Außerdem

können Sie auf der Seite www.kaspersky.com einen Überblick über die Virenaktivität erhalten (Link **Überblick über die Virenaktivität**).

SIEHE AUCH

Update-Einstellungen 52

START UND BEENDEN DER UPDATEAUFGABE

Gehen Sie folgendermaßen vor, um die Updateaufgabe zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf der Registerkarte **Update** auf **Update ausführen**. Klicken Sie auf die Schaltfläche **Update abbrechen** falls eine laufende Aufgabe beendet werden soll.

   Der Fortschritt und das Ergebnis der Ausführung von der Updateaufgabe werden im folgenden Fenster dargestellt.

SIEHE AUCH

Update 31

ROLLBACK ZUM VORHERIGEN UPDATE

Gehen Sie folgendermaßen vor, um zur Verwendung der vorhergehenden Version der Datenbanken zurückzukehren:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf der Registerkarte **Update** auf **Rollback zu den vorherigen Datenbanken**. Das Fenster **Update-Rollback** wird geöffnet.
3. Klicken Sie im folgenden Fenster auf **Letztes Update rückgängig machen**.

SIEHE AUCH

Update 31

QUARANTÄNE UND BACKUP

Dieser Abschnitt informiert über die Quarantäne und das Backup.

IN DIESEM ABSCHNITT

QUARANTÄNE

Die *Quarantäne* ist ein spezieller Speicher, in den Objekte verschoben werden, die möglicherweise von Viren infiziert sind.

Möglicherweise infizierte Objekte sind Objekte, die verdächtig sind, von Viren oder Virenmodifikationen infiziert zu sein. Ein solches Objekt kann während der Virensuche gefunden und in die Quarantäne verschoben werden.

Objekte werden in folgenden Fällen während der Virensuche in die Quarantäne verschoben:

- Der Code des analysierten Objekts besitzt Ähnlichkeit mit einer bekannten Bedrohung, wurde aber teilweise verändert.

  Die Datenbanken von Kaspersky Rescue Disk enthalten jene Bedrohungen, die bisher von den Kaspersky-Lab-Spezialisten untersucht wurden. Wenn ein Schadprogramm verändert wird und diese Veränderungen noch nicht in die Signaturen aufgenommen wurden, klassifiziert Kaspersky Rescue Disk das Objekt, das von einem veränderten Schadprogramm infiziert ist, als möglicherweise infiziertes Objekt und informiert darüber, welcher Bedrohung diese Infektion ähnelt.

- Der Code des gefundenen Objekts erinnert an die Struktur eines Schadprogramms. Die Bedrohungssignaturen enthalten jedoch keine entsprechenden Einträge.

  Es ist durchaus möglich, dass es sich um eine neue Art von Bedrohung handelt. Deshalb klassifiziert Kaspersky Rescue Disk dieses Objekt als möglicherweise infiziertes Objekt.

Der Verdacht, dass eine Datei durch einen Virus infiziert ist, wird mit dem heuristischen Code Analysator ermittelt, mit dessen Hilfe bis zu 92 % neuer Viren erkannt werden. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Ein Objekt unter Quarantäne zu stellen, bedeutet, es wird nicht kopiert, sondern verschoben: Das Objekt wird am ursprünglichen Speicherort gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar. Sie können die Einstellungen für Quarantäne anpassen (siehe Abschnitt "Quarantäne- und Backup-Objekte speichern" auf S. 63).

Mit Objekten, die in die Quarantäne verschoben wurden, können Sie folgende Aktionen ausführen:

- Dateien, die Sie für infiziert halten, in die Quarantäne verschieben.
- Mit Hilfe der aktuellen Datenbanken von Kaspersky Rescue Disk untersuchen und desinfizieren.

- Dateien wiederherstellen entweder in einem vom Benutzer gewählten Ordner oder in den Ordnern, aus denen sie (standardmäßig) in die Quarantäne verschoben wurden.
- Ein beliebiges Quarantäneobjekt oder eine Gruppe ausgewählter Objekte löschen.

Sie können die Aktion mit Objekten in der Quarantäne ändern (auf S. 34).

SIEHE AUCH

AKTION MIT OBJEKTEN IN DER QUARANTÄNE

Gehen Sie folgendermaßen vor, um Aktionen in Bezug auf Quarantäneobjekte auszuführen:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Quarantäne**. Das Fenster **Schutzstatus** wird geöffnet.
3. Wählen Sie im folgenden Fenster auf der Registerkarte **Erkannte Bedrohungen** ein Objekt und öffnen Sie durch Rechtsklick das Kontextmenü.
4. Wählen Sie eine Aktion für das Objekt:
   - **Untersuchen** – Objekte untersuchen, die vom Benutzer in die Quarantäne verschoben wurden.
   - **Aus der Liste löschen** – Der Eintrag über den Fund des Objekts wird aus dem Bericht gelöscht. Beim Löschen eines Objekts aus der Liste wird es auch aus dem Backup entfernt.
   - **Wiederherstellen** – Das Objekt wird wiederhergestellt.
   - **Alle desinfizieren** – Alle Objekte der Liste desinfizieren. Die Anwendung versucht, die Objekte unter Verwendung der Virendatenbanken zu verarbeiten.

     Diese Aktion ist nur für aktive Bedrohungen verfügbar.
   - **Liste leeren** – die Liste der gefundenen Objekte wird geleert. Ihnen wird vorgeschlagen, die Objekte aus der Liste und aus dem Backup zu entfernen.

     Die Objekte nur aus der Liste zu entfernen ist nicht möglich.

SIEHE AUCH

BACKUP

Bei der Desinfektion von Objekten kann es vorkommen, dass es nicht gelingt, die Objekte vollständig zu erhalten. Wenn ein desinfiziertes Objekt wichtige Informationen enthielt, die aufgrund der Desinfektion vollständig oder teilweise verloren gingen, kann versucht werden, das ursprüngliche Objekt über seine Sicherungskopie wiederherzustellen.

Eine *Sicherungskopie* ist eine Kopie des gefährlichen Originalobjekts. Sie wird bei der ersten Desinfektion oder beim Löschen des Objekts erstellt und im Backup gespeichert.

Das *Backup* ist ein spezieller Speicher für Sicherungskopien gefährlicher Objekte, die verarbeitet oder gelöscht werden. Die wichtigste Funktion des Backups besteht in der Möglichkeit, das ursprüngliche Objekt jederzeit wiederherzustellen. Die Sicherungskopien werden im Backup in einem speziellen Format gespeichert und stellen keine Gefahr dar. Sie können die Einstellungen für das Speichern der Backup-Objekte ändern (siehe Abschnitt "Quarantäne- und Backup-Objekte speichern" auf S. 63).

SIEHE AUCH

BERICHTE

Dieser Abschnitt enthält Informationen über Berichte und die Arbeit damit.

IN DIESEM ABSCHNITT

BERICHTE

Die Ausführung jeder Aufgabe zur Untersuchung von Objekten und jeder Updateaufgabe wird in einem Bericht protokolliert. Hier wird angezeigt, wie viele gefährliche und verdächtige Objekte vom Programm während eines bestimmten Zeitraums gefunden wurden.

Bei der Arbeit mit Berichten können Sie folgende Aktionen ausführen:

- Aufgabe auswählen (siehe S. 37), für die ein Ereignisbericht angezeigt werden soll.
- Anordnung der Daten verwalten (siehe S. 37).

  Sie können die Anordnung der Daten, die in einem Bericht enthalten sind, verwalten. Dazu können die Daten nach verschiedenen Merkmalen sortiert werden.
- Wählen Sie einen Ereignistyp (siehe S. 38), nach dem der Bericht angeordnet werden soll.

  Eine vollständige Liste aller wichtigen Ereignisse, die bei der Ausführung einer Untersuchungsaufgabe oder einer Updateaufgabe für die Programm-Datenbanken auftreten, wird im Bericht protokolliert. Sie können den Typ der Ereignisse wählen, die im Bericht angezeigt werden sollen.
- Darstellung von Daten auf dem Bildschirm verwalten (siehe S. 39).

  Die im Bericht enthaltenen Ereignisse werden in Tabellenform dargestellt. Sie können steuern, welche Informationen angezeigt werden sollen, indem Sie Beschränkungsbedingungen angeben.
- Auswählen, in welcher Form (siehe S. 44) die statistischen Informationen auf dem Bildschirm dargestellt werden sollen.

  Im unteren Bereich des Berichtsfensters befindet sich eine Statistik für die Aufgaben von Kaspersky Rescue Disk.
- Bericht in einer Datei speichern (siehe S. 41).

- Komplexe Filterbedingungen (siehe S. 42) festlegen.

  Sie können die Intervalle für die Datensuche in einer beliebigen Spalte der Tabelle festlegen. Der Datenzugriff mit Hilfe eines komplexen Filters basiert auf den logischen Operationen Konjunktion (logisches **UND**) und Disjunktion (logisches **ODER**), mit deren Hilfe sich der Datenzugriff steuern lässt.

- Suche nach Ereignissen (siehe S. 43) ausführen, die im System eingetreten und vom Programm verarbeitet wurden.

Die Ausführung der Aufgabe zur Untersuchung von Objekten und der Update-Aufgabe wird auch im Abschnitt Statistik festgehalten (siehe Abschnitt "Erweiterte Statistikanzeige" auf S. 44). Sie können die Statistik als Grafik oder in Tabellenform darstellen lassen (abhängig von der Aufgabe). Für den Wechsel zur erweiterten Statistik dient die Schaltfläche im oberen Bereich des Fensters. Sie können erfahren, wie viele gefährliche und verdächtige Objekte bei der Arbeit des Programms gefunden wurden, wie viele davon desinfiziert, gelöscht oder in die Quarantäne gestellt wurden.

SIEHE AUCH

Berichte und Speicher 60

AUFGABE FÜR DAS ERSTELLEN EINES BERICHTS WÄHLEN

Gehen Sie folgendermaßen vor, um einen Bericht über eine bestimmte Aufgabe zu erhalten:

1. Öffnen Sie das Programmhauptfenster.
2. Betätigen Sie im oberen Bereich des Fensters den Link **Bericht**. Das Fenster **Schutzstatus** wird geöffnet.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
4. Wählen Sie im folgenden Fenster links oben in der Dropdown-Liste eine Aufgabe aus, für die ein Bericht erstellt werden soll (s. Abb. unten).

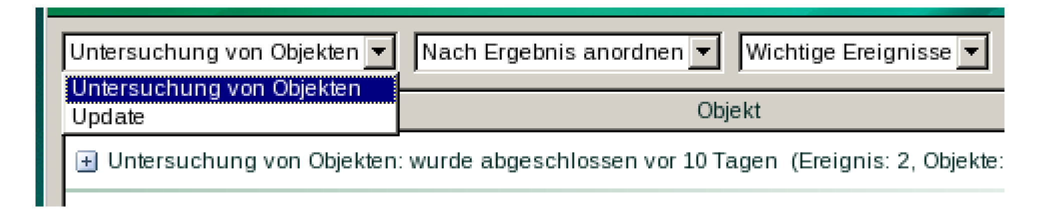


Abbildung 7. Aufgabe für das Erstellen eines Berichts wählen

SIEHE AUCH

Berichte 36

ANORDNUNG VON INFORMATIONEN IM BERICHT

➡ *Gehen Sie folgendermaßen vor, um die Anordnung nach einen bestimmten Merkmal zu verwenden:*

1. Öffnen Sie das Programmhauptfenster.
2. Betätigen Sie im oberen Bereich des Fensters den Link **Bericht**. Das Fenster **Schutzstatus** wird geöffnet.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.
4. Wählen Sie im folgenden Fenster in der Dropdown-Liste (s. Abb. unten) das Kriterium für die Sortierung:
   - **Unsortiert** – es erfolgt keine Sortierung der Ereignisse.
   - **Nach Untersuchungsergebnis anordnen** – die Daten werden nach den Ergebnissen der Untersuchung oder Verarbeitung eines Objekts angeordnet.

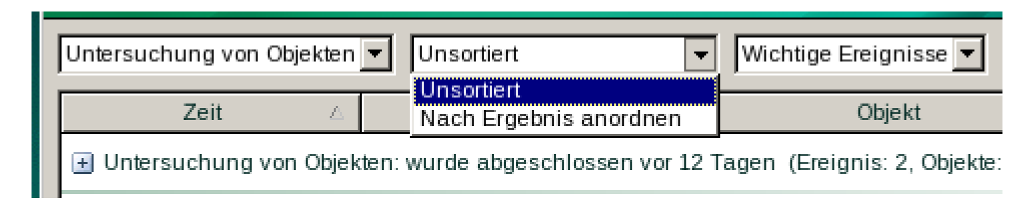


Abbildung 8. Auswahl der Sortierung

Zur Vereinfachung und Verkleinerung der Gruppierung ist eine Suche nach einem Schlüsselwort vorgesehen (s. Abschnitt "Suche nach Ereignissen" auf S. 43). Außerdem können Sie Suchkriterien festlegen.

SIEHE AUCH

EREIGNISTYP AUSWÄHLEN

➡ *Gehen Sie folgendermaßen vor, um einen Ereignistyp auszuwählen, für den ein Bericht erstellt werden soll:*

1. Öffnen Sie das Programmhauptfenster.
2. Betätigen Sie im oberen Bereich des Fensters den Link **Bericht**. Das Fenster **Schutzstatus** wird geöffnet.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.

4. Wählen Sie im folgenden Fenster rechts in der Dropdown-Liste (s. Abb. unten) einen Ereignistyp:

   - **Kritische Ereignisse** – Ereignisse mit kritischer Priorität, die auf Probleme bei der Arbeit von Kaspersky Rescue Disk oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Dazu zählen beispielsweise ein Virenfund oder eine Funktionsstörung.
   - **Wichtige Ereignisse** – Ereignisse, die unbedingt beachtet werden müssen, weil sie auf Situationen bei der Programmarbeit hinweisen, die Ihre Reaktion erfordern (z.B. Ereignis **wurde abgebrochen**).
   - **Alle Ereignisse** – wenn ein Bericht über alle Ereignisse erstellt werden soll.

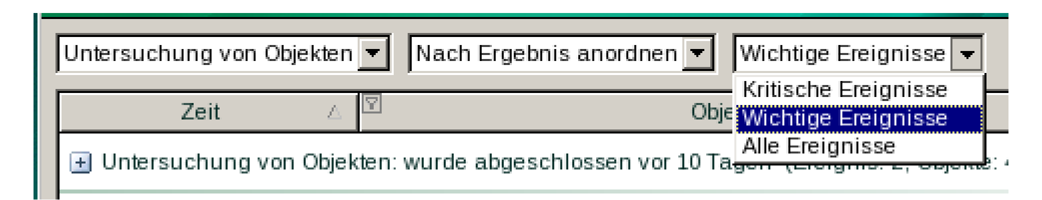


Abbildung 9. Ereignistyp auswählen

Bei Auswahl des Punkts **Alle Ereignisse** werden im Bericht alle Ereignisse angezeigt, wenn im Abschnitt **Berichte und Speicher** im Block **Berichte** das Kontrollkästchen aktiviert ist (siehe Abschnitt "Aufnahme unkritischer Ereignisse in den Bericht" auf S. 62), das die Protokollierung unkritischer Ereignisse im Bericht erlaubt. Wenn dieses Kontrollkästchen nicht aktiviert ist, werden neben der Dropdown-Liste, die der Auswahl von Ereignistypen dient, ein Warnsymbol und der Link **Deaktiviert** angezeigt. Verwenden Sie diesen Link, um in das Fenster zum Anpassen von Berichten zu gehen und die entsprechenden Kontrollkästchen zu aktivieren.

SIEHE AUCH

Berichte 36

DARSTELLUNG VON DATEN AUF DEM BILDSCHIRM

➨ *Gehen Sie folgendermaßen vor, um die Darstellung von Daten auf dem Bildschirm zu ändern:*

1. Öffnen Sie das Programmhauptfenster.
2. Betätigen Sie im oberen Bereich des Fensters den Link **Bericht**. Das Fenster **Schutzstatus** wird geöffnet.

3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht** und passen Sie die Darstellung von Daten an:

   - Um eine Beschränkungsbedingung festzulegen, führen Sie links von der Überschrift der Tabellenspalte, für die eine Beschränkung festgelegt werden soll, einen Linksklick aus (s. Abb. unten). Wählen Sie in der Dropdown-Liste die erforderliche Beschränkung. Bei Auswahl des Punkts **Benutzerdefiniert** können Sie komplexe Filterbedingungen angeben (siehe Abschnitt "Verwendung der komplexen Filterung" auf S. 42). Wenn alle Daten angezeigt werden sollen, wählen Sie in der Beschränkungsliste den Punkt **Alle** aus.

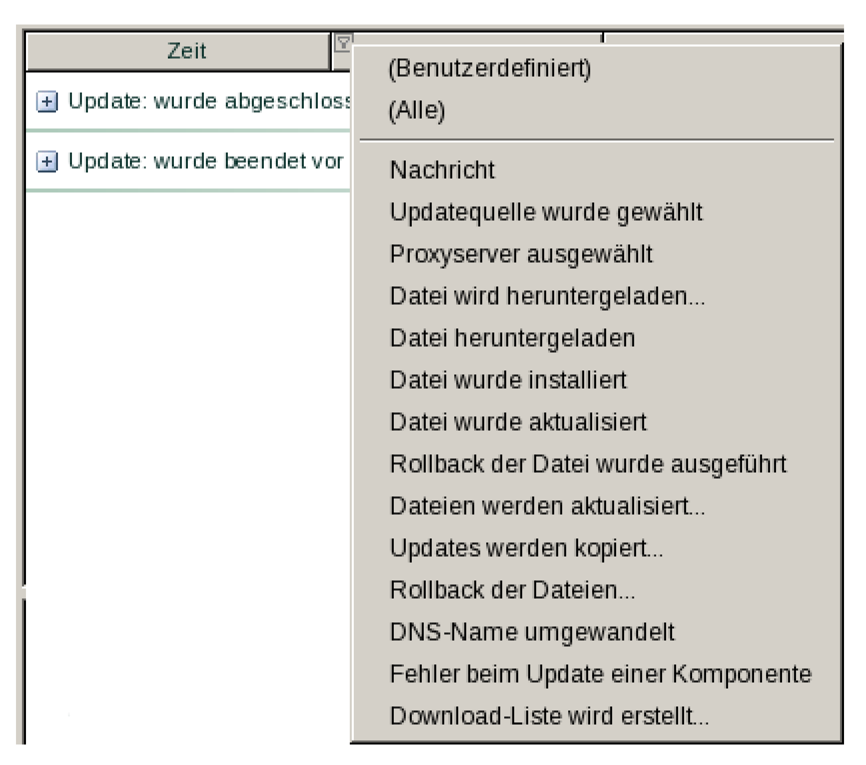


Abbildung 10. Beschränkungsbedingung festlegen

   - Klicken Sie auf das Symbol ⊞ links von der Benennung des Ereignisses, um ausführliche Informationen zum Ereignis zu erhalten. Sie können die Darstellung der Daten ändern. Klicken Sie hierzu mit der rechten Maustaste rechts neben der Überschrift einer beliebigen Spalte und wählen Sie im Kontextmenü die Art der Sortierung aus (s. Abb. unten).

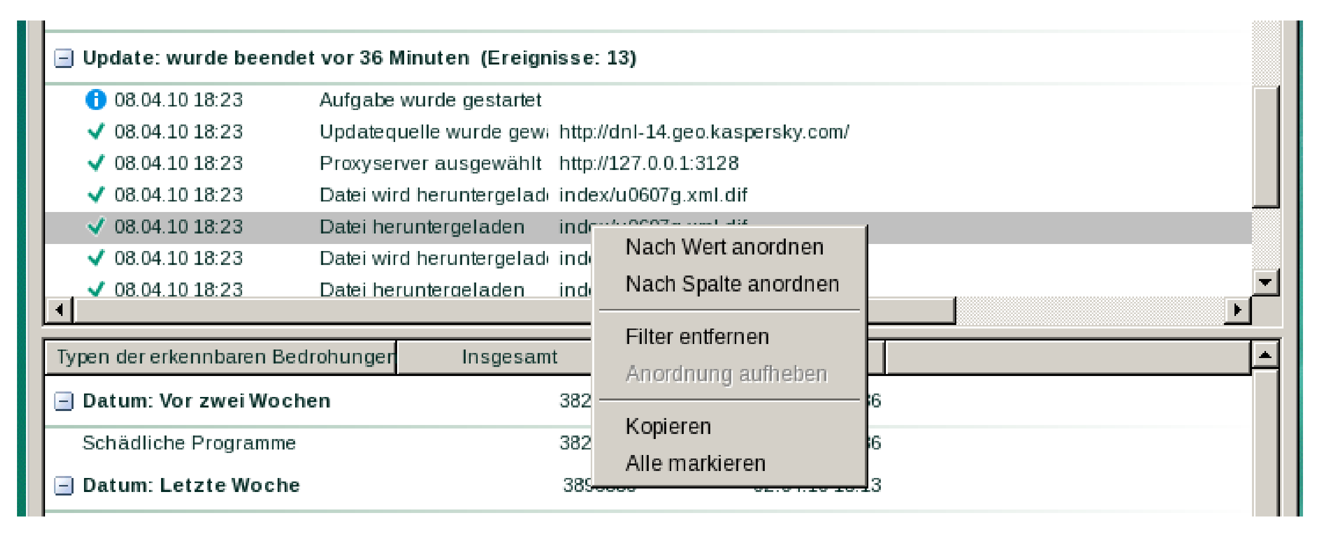


Abbildung 11. Auswahl der Darstellung der Daten

- Um die Spalten einer Tabelle auszublenden / einzublenden, klicken Sie mit der rechten Maustaste im folgenden Fenster rechts von der Überschrift einer beliebigen Tabellenspalte und deaktivieren Sie im Kontextmenü die Kontrollkästchen der entsprechenden Bezeichnungen (s. Abb. unten).

- Das Kontextmenü der Spalte ermöglicht schnellen Zugriff auf ein beliebiges Merkmal, das die Anordnung und Auswahl von Ereignissen erlaubt (s. Abb. unten).

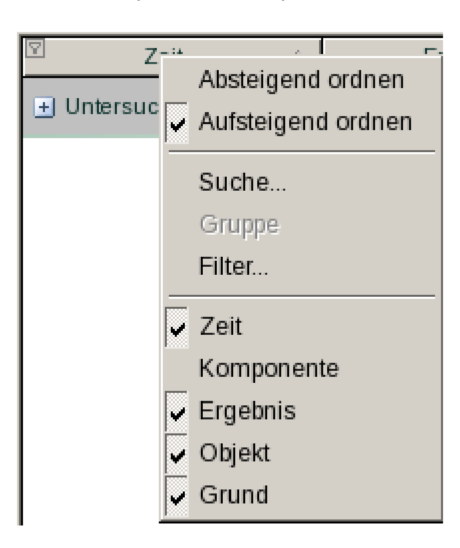


Abbildung 12. Menü zur Gruppierung und Auswahl von Ereignissen

- Klicken Sie links vom Namen der entsprechenden Spalte auf das Symbol ⊞, (s. Abb. unten), damit alle Elemente der Tabellenspalte angezeigt werden. Die Überschrift der geöffneten Spalten enthält einen Pfeil, der die Anordnungsreihenfolge anzeigt. Sie können die Anordnung mit Hilfe des Pfeilsymbols ändern.



Abbildung 13. Tabellenspalten vollständig anzeigen

SIEHE AUCH

BERICHT IN DATEI SPEICHERN

➧ *Gehen Sie folgendermaßen vor, um einen Bericht in einer Datei zu speichern:*

1. Öffnen Sie das Programmhauptfenster.
2. Betätigen Sie im oberen Bereich des Fensters den Link **Bericht**. Das Fenster **Schutzstatus** wird geöffnet.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**. Das gleichnamige Fenster wird geöffnet.

4. Erstellen Sie den gewünschten Bericht und klicken Sie auf die Schaltfläche **Speichern**.

5. Geben Sie den Ordner, in dem die Berichtsdatei gespeichert werden soll, und den Dateinamen an.

SIEHE AUCH

Berichte 36

VERWENDUNG DER KOMPLEXEN FILTERUNG

Gehen Sie folgendermaßen vor, um komplexe Filterbedingungen festzulegen:

1. Öffnen Sie das Programmhauptfenster.

2. Betätigen Sie im oberen Bereich des Fensters den Link **Bericht**. Das Fenster **Schutzstatus** wird geöffnet.

3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**. Das gleichnamige Fenster wird geöffnet.

4. Führen Sie links von der Überschrift der Tabellenspalte, für die komplexe Filterbedingungen festgelegt werden sollen, einen Linksklick aus. Wählen Sie im Kontextmenü den Punkt **Benutzerdefiniert** (s. Abb. unten). Außerdem können Sie auf den Punkt **Filter** im Kontextmenü (s. Abschnitt "Darstellung von Daten auf dem Bildschirm" auf S. 39) gehen, der mit einem Klick auf die rechte Maustaste auf die gewünschte Tabellenspalte verfügbar wird.

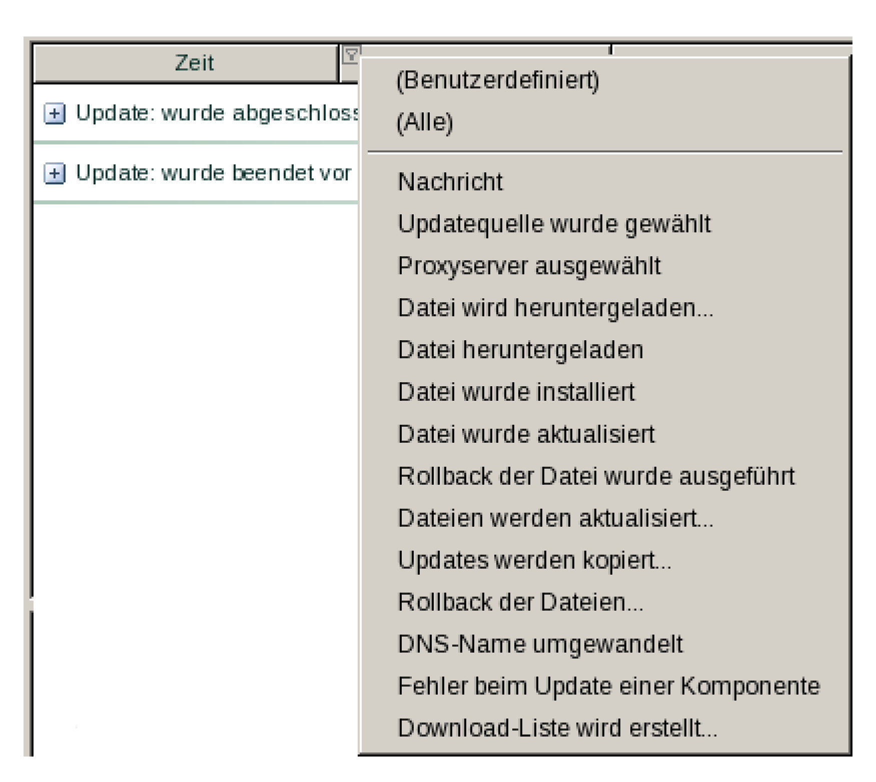


Abbildung 14. Beschränkungsbedingung festlegen

5. Legen Sie im folgenden Fenster Benutzerdefinierter **Filter** die erforderlichen Filterbedingungen fest.

   In den Feldern, die sich auf der rechten Seite des Fensters befinden, werden die Grenzen des Zugriffs angegeben. Auf der linken Fensterseite, in der Dropdown-Liste **Bedingung**, werden die Zugriffsbedingungen für Ereignisse gewählt. **Größer** bedeutet beispielsweise größer als der im Feld rechts angegebene Wert.

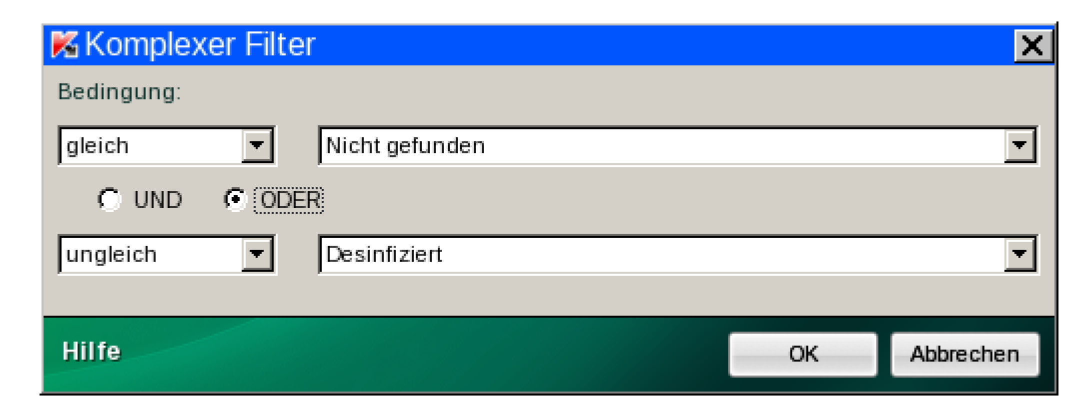


Abbildung 15. Komplexe Filterbedingungen festlegen

   Wenn Sie möchten, dass er Datenzugriff beide festgelegte Bedingungen erfüllt, wählen Sie **UND**. Ist eine Bedienung ausreichend, dann wählen Sie **ODER**.

   Für bestimmte Spalten gilt kein Zahlen- oder Zeitwert als Grenze des Suchintervalls, sondern ein Wort (z.B. das Untersuchungsergebnis **OK** für die Spalte **Ergebnis**). In diesem Fall wird das als Grenze angegebene Wort dem Alphabet nach mit den anderen Wortwerten für die gewählte Spalte verglichen.

SIEHE AUCH

Berichte 36

SUCHE NACH EREIGNISSEN

Gehen Sie folgendermaßen vor, um die Ereignissuche zu verwenden:

1. Öffnen Sie das Programmhauptfenster.
2. Betätigen Sie im oberen Bereich des Fensters den Link **Bericht**. Das Fenster **Schutzstatus** wird geöffnet.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.

4. Führen Sie im folgenden Fenster rechts von der Überschrift einer beliebigen Tabellenspalte einen Rechtsklick aus. Wählen sie im folgenden Menü den Punkt **Suche**.

5. Legen Sie im folgenden Fenster **Suche** (s. Abb. unten) die Suchkriterien fest.

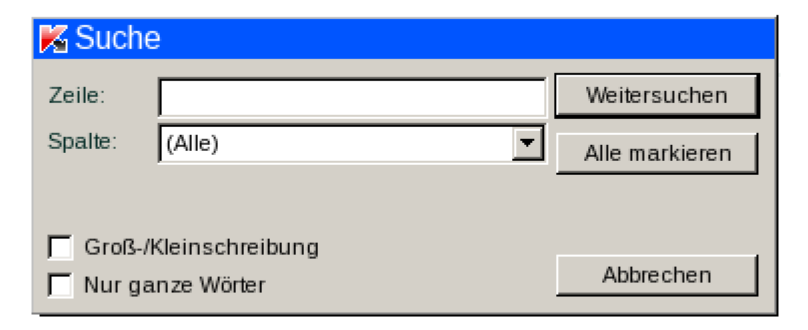


Abbildung 16. Suchfenster

SIEHE AUCH

Berichte 36

ERWEITERTE STATISTIKANZEIGE

Gehen Sie folgendermaßen vor, um eine erweiterte Statistik anzuzeigen:

1. Öffnen Sie das Programmhauptfenster.

2. Betätigen Sie im oberen Bereich des Fensters den Link **Bericht**. Das Fenster **Schutzstatus** wird geöffnet.

3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Vollständiger Bericht**.

4. Wählen Sie im folgenden Fenster eine Aufgabe, für die eine erweiterte Statistik angezeigt werden soll, und klicken Sie auf im oberen Bereich des Fensters.

SIEHE AUCH

Berichte 36

Erweiterte Programmeinstellungen

Dieser Abschnitt enthält Informationen über die Konfiguration von Kaspersky Rescue Disk.

In diesem Abschnitt

Untersuchung von Objekten

Dieser Abschnitt enthält Informationen darüber, wie die Parameter der Aufgabe zur Untersuchung von Objekten auf Ihrem Computer zu konfigurieren sind.

In diesem Abschnitt

UNTERSUCHUNGSEINSTELLUNGEN FÜR OBJEKTE

Auf welche Weise die Untersuchung von Objekten auf Ihrem Computer erfolgt, wird durch eine Auswahl von Parametern bestimmt, die für diese Aufgabe festgelegt werden.

Um die Aufgabe zur Untersuchung von Objekten einzurichten, können Sie wie folgt vorgehen:

- Sicherheitsstufe ändern (siehe Abschnitt "Ändern der Sicherheitsstufe" auf S. 47).

  Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Untersuchungsparametern verstanden. Die Spezialisten von Kaspersky Lab haben die drei folgenden Sicherheitsstufen vordefiniert:

  - **Hoch** - Untersuchung des gesamten Computers oder eines Laufwerks, Ordners oder einer Datei des Computers mit maximaler Ausführlichkeit.
  - **Empfohlen** - die Parameter umfassen die Untersuchung der gleichen Objekte wie auf der Stufe **Hoch**, unter Ausnahme von Dateien in Mailformaten.
  - **Niedrig** - Stufe, die weniger Arbeitsspeicher erfordert, da die Auswahl der zu untersuchenden Dateien auf dieser Stufe eingeschränkt wird.

  Bei der Entscheidung darüber, welche Sicherheitsstufe Sie wählen, sollten Sie die aktuelle Situation berücksichtigen.

- Dateitypen, die auf Viren untersucht werden sollen, festlegen (siehe Abschnitt "Ändern des Typs der zu untersuchenden Objekte" auf S. 48).

  Kaspersky Rescue Disk untersucht standardmäßig nur potentiell infizierbare Dateien. Sie können den Schutzbereich erweitern oder einschränken, indem Sie die Typen der zu untersuchenden Dateien ändern. Sie können beispielsweise nur exe-Dateien, die von Wechseldatenträgern aus gestartet werden, untersuchen lassen. Allerdings sollten Sie sicherstellen, dass eine Einschränkung des Schutzbereichs nicht zu einem Sicherheitsrisiko für Ihren Computer führt.

- Untersuchungsdauer beschränken (siehe Abschnitt "Beschränkung der Untersuchungsdauer" auf S. 49).

  Die Untersuchungsdauer kann für jede Datei beschränkt werden. Nach Ablauf der festgelegten Zeit, wird die Dateiuntersuchung abgebrochen.

- Parameter für die Untersuchung zusammengesetzter Dateien anpassen (siehe S. 49).

  Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

  Sie können den Typ der zusammengesetzten Dateien festlegen, die untersucht werden sollen. Außerdem können Sie festlegen, bis zu welcher maximalen Größe eine zusammengesetzte Datei untersucht werden soll. Zusammengesetzte Dateien, die die festgelegte Größe überschreiten, werden nicht untersucht.

- Untersuchungsmethode wählen (siehe Abschnitt "Untersuchungsmethode ändern" auf S. 50), die die Ausführlichkeit der Untersuchung beeinflusst.

  Sie können die Untersuchungsparameter anpassen, die die Ausführlichkeit der Untersuchung beeinflussen. In der Grundeinstellung ist der Untersuchungsmodus mit Hilfe der Einträge in den Datenbanken des Programms immer aktiviert.

  Die Datenbanken werden von den Kaspersky-Lab-Spezialisten gepflegt. Die Datenbanken enthalten eine genaue Beschreibung aller momentan existierenden Bedrohungen der Computersicherheit sowie Methoden zu ihrer Identifikation und Desinfektion. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen. Um die Erkennungsqualität für Bedrohungen zu steigern, empfehlen wir, regelmäßig Updates für die Datenbanken von den Kaspersky-Lab-Updateservern herunterzuladen.

Der Suchmodus, in dem Kaspersky Rescue Disk ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht, heißt *Signaturanalyse* und wird immer verwendet. Außerdem können Sie die *heuristische Analyse* verwenden. Diese Methode umfasst die Analyse der Aktivität, die ein Objekt im System zeigt. Wenn diese Aktivität als typisch für schädliche Objekte gilt, lässt sich ein Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen.

Zusätzlich kann die Genauigkeitsstufe der heuristischen Analyse ausgewählt werden: **oberflächlich**, **mittel** oder **tief**. Bewegen Sie dazu den Schieberegler auf die gewünschte Position.

- Aktion beim Fund einer Bedrohung festlegen (siehe Abschnitt "Ändern der Aktion beim Fund einer Bedrohung" auf S. 48).

  Beim Fund einer Bedrohung weist Kaspersky Rescue Disk dieser einen der folgenden Statusvarianten zu:

  - Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
  - Status *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise wurde in der Datei der Codes eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden.

  Wenn Kaspersky Rescue Disk bei einer Untersuchung infizierte oder möglicherweise infizierte Objekte findet, werden Sie darüber informiert. Auf dem Fund einer Bedrohung muss reagiert werden, indem eine Aktion für das Objekt ausgewählt wird. Standardmäßig ist in Kaspersky Rescue Disk als Aktion für ein gefundenes Objekt die Variante **Aktion nach Abschluß der Untersuchung erfragen** festgelegt. Sie können die Aktion ändern.

- Zu den empfohlenen Einstellungen zurückkehren (siehe Abschnitt "Standardmäßige Untersuchungseinstellungen wiederherstellen" auf S. 51).

  Diese Parameter gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

SIEHE AUCH

Virensuche 28

SICHERHEITSSTUFE ÄNDERN

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Es öffnet sich der Abschnitt **Untersuchung von Objekten**.
3. Wählen Sie im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe:

   - **Hoch** - vollständige Untersuchung des gesamten Computers oder eines Laufwerks, Ordners oder einer Datei des Computers.
   - **Empfohlen** - die Parameter umfassen die Untersuchung der gleichen Objekte wie auf der Stufe **Hoch**, unter Ausnahme von Dateien in Mailformaten.
   - **Niedrig** - Stufe, die weniger Arbeitsspeicher erfordert, da die Auswahl der zu untersuchenden Dateien auf dieser Stufe eingeschränkt wird.

Wenn keine der vordefinierten Stufen Ihren Anforderungen entspricht, können Sie die Untersuchungsparameter anpassen. Dadurch ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**. Um die standardmäßigen Untersuchungsparameter wiederherzustellen, wählen Sie eine der vordefinierten Stufen oder klicken Sie auf **Standard**.

SIEHE AUCH

Untersuchungseinstellungen für Objekte 45

AKTION BEIM FUND EINER BEDROHUNG ÄNDERN

Bevor ein Desinfektionsversuch erfolgt oder ein Objekt gelöscht wird, legt Kaspersky Rescue Disk eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Es öffnet sich der Abschnitt **Untersuchung von Objekten**.
3. Wählen Sie im Block **Aktion** eine der folgenden Aktionen:
   - **Aktion nach Abschluß der Untersuchung erfragen** – Kaspersky Rescue Disk verschiebt die Verarbeitung der Objekte bis zum Abschluss der Untersuchung.
   - **Aktion sofort erfragen** – das Programm zeigt eine Warnmeldung auf dem Bildschirm an, die darüber informiert, welchen schädlichen Code das infizierte / möglicherweise infizierte Objekt enthält, und bietet Aktionen zur Auswahl an.
   - **Aktion ausführen**:
     - **Desinfizieren** – Kaspersky Rescue Disk führt einen Desinfektionsversuch mit dem gefundenen Objekt aus, ohne nach einer Bestätigung zu fragen. Möglicherweise infizierte Objekte werden in die Quarantäne verschoben. Informationen darüber werden im Bericht aufgezeichnet. Später kann versucht werden, das Objekt zu desinfizieren.
     - **Löschen, wenn Desinfektion nicht möglich** – Kaspersky Rescue Disk führt einen Desinfektionsversuch mit dem gefundenen Objekt aus, ohne nach einer Bestätigung zu fragen. Irreparable Objekte werden gelöscht, möglicherweise infizierte Objekte werden in die Quarantäne verschoben.

SIEHE AUCH

Untersuchungseinstellungen für Objekte 45

TYP DER ZU UNTERSUCHENDEN OBJEKTE ÄNDERN

Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Es öffnet sich der Abschnitt **Untersuchung von Objekten**.

3. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Bestimmen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Dateitypen** das Format und die Erweiterung der Dateien, die beim Ausführen der gewählten Aufgabe untersucht werden sollen:

   - **Alle Dateien** – in diesem Fall werden alle Dateien ohne Ausnahme einer Untersuchung unterzogen.

   - **Dateien nach Format untersuchen** – bei der Auswahl dieser Gruppe untersucht Kaspersky Rescue Disk nur potentiell infizierbare Dateien**,** d.h. Dateien, in die ein Virus eindringen kann. Vor der Untersuchung eines Objekts wird seine interne Kopfzeile im Hinblick auf das Dateiformat (txt, doc, exe usw.) analysiert.

   - **Dateien nach Erweiterung untersuchen** – in diesem Fall untersucht Kaspersky Rescue Disk nur potentiell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt.

Es sollte beachtet werden, dass das Risiko des Eindringens von schädlichem Code in die Dateien bestimmter Formate (z.B. txt) und die spätere Aktivierung relativ gering ist. Gleichzeitig ist die Gefahr des Eindringens von Schadcode in Dateien, die ausführbaren Code enthalten oder enthalten können (z.B. exe, dll, doc) relativ hoch.

Es sollte beachtet werden, dass ein Angreifer einen Virus in einer Datei mit der Erweiterung txt an Ihren Computer senden kann, obwohl es sich in Wirklichkeit um eine ausführbare Datei handelt, die in eine txt-Datei umbenannt wurde. Wenn Sie die Variante **Dateien nach Erweiterung untersuchen** wählen, wird eine solche Datei bei der Untersuchung übersprungen. Wenn Sie die Variante **Dateien nach Format untersuchen** gewählt haben, analysiert der Dateischutz ungeachtet der Erweiterung die Kopfzeile der Datei, wodurch sich ergibt, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virenuntersuchung unterzogen.

SIEHE AUCH

Untersuchungseinstellungen für Objekte.. 45

BESCHRÄNKUNG DER UNTERSUCHUNGSDAUER

Gehen Sie folgendermaßen vor, um die Untersuchungsdauer einzuschränken:

1. Öffnen Sie das Programmhauptfenster.

2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Es öffnet sich der Abschnitt **Untersuchung von Objekten**.

3. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung optimieren** das Kontrollkästchen ☑ **Dateien überspringen, wenn Untersuchung länger als** und geben Sie im Feld daneben die Untersuchungsdauer an. Nach Ablauf der festgelegten Zeit, wird die Dateiuntersuchung abgebrochen.

SIEHE AUCH

Untersuchungseinstellungen für Objekte.. 45

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

➡ *Um Parameter für die Untersuchung von zusammengesetzten Dateien anzupassen, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster.

2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Es öffnet sich der Abschnitt **Untersuchung von Objekten**.

3. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Sie können im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich**, im Block **Untersuchung von zusammengesetzten Dateien**, die folgende Parameter angeben:

   - Der Typ für die zu untersuchenden zusammengesetzten Dateien. Dazu aktivieren Sie die entsprechenden Kontrollkästchen.

   - Die maximale Größe für zusammengesetzte Dateien, die untersucht werden sollen. Klicken Sie dazu auf **Erweitert**. Aktivieren Sie im folgenden Fenster **Zusammengesetzte Dateien** das Kontrollkästchen ☑ **Große zusammengesetzte Dateien nicht entpacken** und legen Sie darunter im Feld die maximale Größe für zu untersuchende Dateien fest. Zusammengesetzte Dateien, die den Grenzwert überschreiten, werden nicht untersucht.

     Wenn das Kontrollkästchen ☑ **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist und die Größe einer zusammengesetzten Datei den maximalen festgelegten Wert nicht überschreitet, erfolgt die Untersuchung der extrahierten Dateien auch dann, wenn ihre Größe den maximalen Wert überschreitet.

SIEHE AUCH

Untersuchungseinstellungen für Objekte.. 45

UNTERSUCHUNGSMETHODE ÄNDERN

➡ *Um die Untersuchungsmethode zu ändern, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster.

2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Es öffnet sich der Abschnitt **Untersuchung von Objekten**.

3. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Gehen Sie im folgenden Fenster auf der Registerkarte **Erweitert**.

5. Im Block **Untersuchungsmethoden** wählen Sie die erforderliche Untersuchungsmethode:

   - ☑ **Signaturanalyse**. Bei der Signaturanalyse werden die Datenbanken von Kaspersky Rescue Disk verwendet, die Beschreibungen der bekannten Bedrohungen und entsprechende Desinfektionsmethoden enthalten. Der Schutz mit Hilfe der Signaturanalyse gewährleistet die minimal erforderliche Sicherheitsstufe. In Übereinstimmung mit den Empfehlungen der Spezialisten von Kaspersky Lab ist diese Analysemethode immer aktiviert.

   - ☑ **Heuristische Analyse**. Die Untersuchung erfolgt auf Basis der Analyse typischer Operationsfolgen, die es erlauben, mit ausreichender Wahrscheinlichkeit auf die Art der Datei zu schließen. Der Vorteil dieser Methode besteht darin, dass neue Bedrohungen bereits erkannt werden, bevor die Virenanalytiker von ihrer Aktivität wissen.

     Zusätzlich können Sie das Genauigkeitsniveau der Untersuchung festlegen: oberflächlich, mittel oder tief. Bewegen Sie dazu den Schieberegler auf die gewünschte Position.

SIEHE AUCH

Untersuchungseinstellungen für Objekte... 45

STANDARDMÄßIGE UNTERSUCHUNGSEINSTELLUNGEN WIEDERHERSTELLEN

➡ *Gehen Sie folgendermaßen vor, um die standardmäßigen Untersuchungseinstellungen für Objekte wiederherzustellen,*

1. Öffnen Sie das Programmhauptfenster.

2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Es öffnet sich der Abschnitt **Untersuchung von Objekten**.

3. Klicken Sie im Block **Sicherheitsstufe** auf **Standard**.

> Sie können jederzeit zu den empfohlenen Einstellungen der Aufgabe zur Untersuchung von Objekten zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

SIEHE AUCH

Untersuchungseinstellungen für Objekte... 45

UPDATE

Dieser Abschnitt enthält Informationen darüber, auf welche Weise die Updateaufgabe auf Ihrem Computer angepasst werden kann.

IN DIESEM ABSCHNITT

UPDATE-EINSTELLUNGEN

Das Update von Kaspersky Rescue Disk wird nach den folgenden Parametern ausgeführt:

Um die Updateaufgabe einzustellen, können Sie folgende Aktionen ausführen:

- Updatequelle auswählen (siehe Abschnitt "Auswahl der Updatequelle" auf S. 52).

  Für die Aktualisierung ist eine Internetverbindung erforderlich.

  Eine *Updatequelle* ist eine Ressource, die Updates der Datenbanken für Kaspersky Rescue Disk enthält. Als Updatequelle können HTTP- oder FTP-Server dienen. Die wichtigste Updatequelle sind standardmäßig die Updateserver von Kaspersky Lab verfügt in mehreren Ländern der Erde. Das sind spezielle Internetseiten, auf denen Updates für alle Kaspersky-Lab-Produkte zur Verfügung stehen. Wenn mehrere Ressourcen als Updatequellen gewählt wurden, greift Kaspersky Rescue Disk bei der Aktualisierung genau nach der Listenreihenfolge darauf zu und aktualisiert sich von der ersten verfügbaren Quelle.

- Regionsoptionen der Updatequelle ändern (siehe Abschnitt "Regionsoptionen der Updatequelle" auf S. 53).

  Die Auswahl des geografisch am nächsten gelegenen Kaspersky-Lab-Updateservers kann die Dauer des Updates verkürzen und die Downloadgeschwindigkeit erhöhen. Sie können den für Sie günstigsten Standort des Servers für den Update-Download wählen.

- Proxyserver-Parameter festlegen (siehe Abschnitt "Parameter des Proxyservers anpassen" auf S. 53).

  Um die Updates von den Servern herunterzuladen, ist eine Verbindung Ihres Computers mit dem Internet erforderlich. In der Grundeinstellung wird die Internetverbindung automatisch ermittelt. Wenn die Internetverbindung über einen Proxyserver erfolgt, passen Sie die Verbindungseinstellungen an (siehe Abschnitt "Parameter des Proxyservers anpassen" auf S. 53).

SIEHE AUCH

Update ....

UPDATEQUELLE AUSWÄHLEN

Für die Aktualisierung ist eine Internetverbindung erforderlich.

Gehen Sie folgendermaßen vor, um eine Updatequelle auszuwählen:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Quelle** auf den Link **Hinzufügen**. Es öffnet sich das Fenster **Auswahl einer Updatequelle**.
5. Wählen Sie im folgenden Fenster eine FTP- oder HTTP-Seite aus oder geben Sie ihre IP-Adresse, den symbolischen Namen oder die URL-Adresse an.

SIEHE AUCH

Update-Einstellungen 52

PARAMETER DES PROXYSERVERS ANPASSEN

Die Updateaufgabe arbeitet standardmäßig mit dem Proxyserver des Systems. Sie können spezielle Proxyserver-Einstellungen für die Updateaufgabe festlegen.

Gehen Sie folgendermaßen vor, um die Proxyserver-Parameter anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Quelle** auf die Schaltfläche **Proxyserver**.
5. Geben Sie im folgenden Fenster die Parameter für den Proxyserver an.

SIEHE AUCH

Update-Einstellungen 52

REGIONSOPTIONEN DER UPDATEQUELLE

➡ *Gehen Sie folgendermaßen vor, um am nächsten gelegenen Server auszuwählen:*

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Quelle** im Block **Regionsoptionen** den Punkt **Aus der Liste auswählen** und wählen Sie aus der Dropdown-Liste das Land, in dem Sie sich gerade aufhalten.

SIEHE AUCH

Update-Einstellungen 52

BEDROHUNGEN UND AUSNAHMEN. VERTRAUENSWÜRDIGE ZONE

Dieser Abschnitt informiert darüber, wie Ihr Computer durch eine Erweiterung der Liste mit erkennbaren Bedrohungen vor unterschiedlichen Malware-Typen geschützt werden kann, wie häufig eingesetzte Programme von der Untersuchung ausgeschlossen werden können und wie Ausnahmeregeln angepasst werden.

IN DIESEM ABSCHNITT

BEDROHUNGEN UND AUSNAHMEN

Kaspersky Rescue Disk bietet Ihnen Schutz vor verschiedenen Arten schädlicher Programme. Unabhängig von den festgelegten Parametern, werden Viren, trojanische Programme und Hackerprogramme immer vom Programm gesucht und neutralisiert. Diese Programme können Ihrem Computer ernsthaften Schaden zufügen. Um die Sicherheit des Computers zu erhöhen, können Sie die Liste der erkennbaren Bedrohungen erweitern. Aktivieren Sie dazu die Kontrolle über unterschiedliche Arten potentiell gefährlicher Programme.

Im Abschnitt **Bedrohungen und Ausnahmen** des Konfigurationsfensters von Kaspersky Rescue Disk können Sie:

- Die Kategorien der erkennbaren Bedrohungen wählen (siehe Abschnitt "Auswahl der Kategorien der erkennbaren Bedrohungen" auf S. 55).
- Eine vertrauenswürdige Zone für die Anwendung anlegen (siehe Abschnitt "Anlegen der vertrauenswürdigen Zone" auf Seite 56).

  Die *vertrauenswürdige Zone* (siehe Abschnitt "*Vertrauenswürdige Zone*" auf S. 55) ist eine benutzerdefinierte Liste von Objekten, die von Kaspersky Rescue Disk nicht kontrolliert werden. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz des Programms.

  Die vertrauenswürdige Zone wird vom Benutzer unter Berücksichtigung der Besonderheiten von Objekten, mit denen er arbeitet, aufgebaut. Das Anlegen einer solchen Liste mit Ausnahmen kann beispielsweise erforderlich sein, wenn Kaspersky Rescue Disk den Zugriff auf ein bestimmtes Objekt blockiert, Sie aber sicher sind, dass dieses Objekt absolut unschädlich ist.

SIEHE AUCH

KATEGORIEN DER ERKENNBAREN BEDROHUNGEN AUSWÄHLEN

Gehen Sie folgendermaßen vor, um die Kategorien erkennbare Bedrohungen auszuwählen:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Gefahren und Ausnahmen** aus.
3. Klicken Sie auf der rechten Fensterseite im Block **Bedrohungen** auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Bedrohungen** die Kontrollkästchen der Bedrohungskategorien, vor denen Sie Ihren Computer schützen möchten.

SIEHE AUCH

VERTRAUENSWÜRDIGE ZONE

Die *vertrauenswürdige Zone* ist eine benutzerdefinierte Liste von Objekten, die von Kaspersky Rescue Disk nicht kontrolliert werden. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz des Programms.

Die vertrauenswürdige Zone wird vom Benutzer unter Berücksichtigung der Besonderheiten von Objekten, mit denen er arbeitet, aufgebaut (siehe Abschnitt "Anlegen der vertrauenswürdigen Zone" auf S. 56). Das Anlegen einer solchen Liste mit Ausnahmen kann beispielsweise erforderlich sein, wenn Kaspersky Rescue Disk den Zugriff auf ein bestimmtes Objekt blockiert, Sie aber sicher sind, dass dieses Objekt absolut unschädlich ist.

Die vertrauenswürdige Zone wird auf Basis der Ausnahmeregeln erstellt (siehe Abschnitt "Erstellen einer Ausnahmeregel" auf S. 57). Eine *Ausnahmeregel* ist eine Kombination von Bedingungen, bei deren Vorhandensein ein Objekt nicht von Kaspersky Rescue Disk untersucht wird.

Sie können einen Typ für den Ausschluss von Dateien aus der Untersuchung angeben:

- **Objekt** – Ein bestimmtes Objekt, ein Ordner oder Dateien, die einer bestimmten Maske entsprechen, werden von der Untersuchung ausgeschlossen.

  > Ein ausgeschlossenes Objekt unterliegt nicht der Untersuchung, wenn das Laufwerk oder der Ordner untersucht wird, auf dem es sich befindet. Wird allerdings ein konkretes Objekt zur Untersuchung ausgewählt, dann wird die Ausnahmeregel ignoriert.

- **Bedrohungstyp** – Ein bestimmtes Objekt, ein Ordner oder Dateien, die einer bestimmten Maske entsprechen, werden von der Untersuchung ausgeschlossen. Ein Objekt wird auf der Grundlage des Status, der ihm nach der Klassifikation der Viren-Enzyklopädie entspricht, von der Untersuchung ausgeschlossen. Der Bedrohungstyp beruht auf der Klassifikation schädlicher und potentiell gefährlicher Programme, die in der Viren-Enzyklopädie von Kaspersky Lab enthalten ist.

  Ein potentiell gefährliches Programm besitzt keine schädliche Funktion, kann aber von einem Schadprogramm als Hilfskomponente benutzt werden, weil es Schwachstellen und Fehler enthält. Zu dieser Kategorie gehören beispielsweise Programme zur Remote-Verwaltung, IRC-Clients, FTP-Server, alle Hilfsprogramme zum Beenden von Prozessen und zum Verstecken ihrer Arbeit, Tastaturspione, Programme zur Kennwortermittlung, Programme zur automatischen Einwahl auf kostenpflichtige Seiten usw. Solche Software wird nicht als Viren klassifiziert (not-a-virus). Sie lässt sich beispielsweise in folgende Typen unterteilen: Adware, Joke, Riskware usw. (ausführliche Informationen über potentiell gefährliche Programme, die von Kaspersky Rescue Disk erkannt werden können, finden Sie in der Viren-Enzyklopädie auf der Seite www.viruslist.com/de). Derartige Programme können aufgrund der Untersuchung gesperrt werden. Da bestimmte Programme dieser Kategorie von vielen Benutzern verwendet werden, besteht die Möglichkeit, potentiell gefährliche Programme von der Untersuchung auszuschließen. Dazu muss zur vertrauenswürdigen Zone der Name oder eine Maske der Bedrohung gemäß der Klassifikation der Viren-Enzyklopädie hinzugefügt werden.

  Es kann beispielsweise sein, dass Sie häufig mit dem Programm Remote Administrator arbeiten. Dabei handelt es sich um ein System, das dem Remote-Zugriff dient und die Arbeit auf einem Remote-Computer erlaubt. Diese Anwendungsaktivität wird von Kaspersky Rescue Disk als potentiell gefährlich eingestuft und kann blockiert werden. Um zu verhindern, dass die Anwendung blockiert wird, muss eine Ausschlussregel mit der Klassifikation RemoteAdmin erstellt werden.

Beim Hinzufügen einer Ausnahme wird eine Regel erstellt, die anschließend bei der Ausführung einer Untersuchung verwendet wird.

SIEHE AUCH

Anlegen der vertrauenswürdigen Zone 56

ANLEGEN DER VERTRAUENSWÜRDIGEN ZONE

Um eine vertrauenswürdige Zone anzulegen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Gefahren und Ausnahmen** aus.

3. Klicken Sie auf der rechten Fensterseite im Block **Ausnahmen** auf **Einstellungen**.

4. Gehen Sie im folgenden Fenster auf der Registerkarte **Regeln für Ausnahmen** folgendermaßen vor:

    - Gelangen Sie über den Link **Hinzufügen**. Das Fenster **Ausnahmeregel** wird geöffnet. Passen Sie im folgenden Fenster die Ausnahmeregel an.

    - Verwenden Sie den Link **Löschen**, um eine Regel aus der Liste zu löschen.

    - Klicken Sie auf den Link **Ändern**, um eine vorhandene Regel zu ändern.

    Regeln können auch vorübergehend von der Untersuchung ausgeschlossen werden, ohne aus der Liste gelöscht zu werden. Markieren Sie dazu die Regel in der Liste und deaktivieren Sie das Kontrollkästchen links vom Namen der Regel.

SIEHE AUCH:

Vertrauenswürdige Zone 55

ERSTELLEN EINER AUSNAHMEREGEL

Gehen Sie folgendermaßen vor, um eine Ausnahmeregel zu erstellen:

1. Öffnen Sie das Programmhauptfenster.

2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Gefahren und Ausnahmen** aus.

3. Klicken Sie auf der rechten Fensterseite im Block **Ausnahmen** auf **Einstellungen**.

4. Klicken Sie im folgenden Fenster auf der Registerkarte **Regeln für Ausnahmen** auf den Link **Hinzufügen**. Das Fenster **Ausnahmeregel** wird geöffnet.

5. Legen Sie im folgenden Fenster im Block **Eigenschaften** einen Ausnahmetyp fest.

SIEHE AUCH

Bedrohungen und Ausnahmen........ 54

ZULÄSSIGE AUSSCHLUSSMASKEN FÜR DATEIEN

Hier werden Beispiele für zulässige Masken genannt, die Sie beim Erstellen der Liste auszuschließender Dateien verwenden können:

1. Masken ohne Dateipfad:

    - ***.exe** – alle Dateien mit der Endung exe;

    - ***.ex?** – alle Dateien mit der Endung *ex?*, wobei anstelle von ? ein beliebiges Zeichen stehen kann;

    - ***test*** – alle Dateien mit dem Namen test.

2. Masken mit absolutem Dateipfad:

   - **/discs/C:/dir/*.*** oder **/discs/C:/dir/*** oder **/discs/C:/dir/** – alle Dateien im Ordner /discs/C:/dir/
   - **/discs/C:/dir/*.exe** – alle Dateien mit der Endung exe im Ordner /discs/C:/dir/;
   - **C:\dir*.ex?** – alle Dateien mit der Endung ex? im Ordner /discs/C:/dir/, wobei anstelle von ? ein beliebiges Zeichen stehen kann;
   - **/discs/C:/dir/test*** – Dateien im Ordner /discs/C:/dir/, die mit test beginnen.

     Damit die Dateien in allen untergeordneten Ordnern des gewählten Ordners von der Untersuchung ausgeschlossen werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen ☑ **Unterordner einschließen**.

3. Masken mit Dateipfad:

   - **dir/*.*** oder **dir/*** oder **dir/** – alle Dateien in allen Ordnern von dir/;
   - **dir/*test*** – alle Dateien test in den Ordnern von dir/;
   - **dir/*.exe** – alle Dateien mit der Endung exe in allen Ordnern von dir/;
   - **dir*.ex?** – alle Dateien mit der Endung ex? in allen Ordnern von dir/, wobei anstelle von ? ein beliebiges Zeichen stehen kann.

     Damit die Dateien in allen untergeordneten Ordnern des gewählten Ordners von der Untersuchung ausgeschlossen werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen ☑ **Unterordner einschließen**.

Die Verwendung der Ausnahmemaske *.* oder * ist nur zulässig, wenn die auszuschließende Bedrohung gemäß der Viren-Enzyklopädie klassifiziert wird. In diesem Fall wird die Bedrohung nicht in allen Objekten gefunden werden. Wenn diese Masken ohne Angabe einer Klassifikation verwendet werden, entspricht dies dem Deaktivieren des Schutzes.

ZULÄSSIGE AUSSCHLUSSMASKEN GEMÄß DER KLASSIFIKATION DER VIREN-ENZYKLOPÄDIE

Wenn als Ausnahme eine Bedrohung mit einem bestimmten Status nach der Klassifikation der Viren-Enzyklopädie hinzugefügt wird, können Sie angeben:

- den vollständigen Namen der Bedrohung, wie er in der Viren-Enzyklopädie auf der Seite www.viruslist.de genannt wird (beispielsweise **not-a-virus:RiskWare.RemoteAdmin.RA.311** oder **Flooder.Win32.Fuxx**).
- den Namen der Bedrohung als Maske, beispielsweise:
  - **not-a-virus*** – Legale, aber potentiell gefährliche Programme sowie Scherzprogramme von der Untersuchung ausschließen.
  - ***Riskware.*** – Alle potentiell gefährlichen Programme des Typs Riskware von der Untersuchung ausschließen.
  - ***RemoteAdmin.*** – Alle Versionen von Programmen zur Fernverwaltung von der Untersuchung ausschließen.

MELDUNGEN

Dieser Abschnitt enthält Informationen darüber, auf welche Weise Parameter für Benachrichtigungen auf Ihrem Computer angepasst werden kann.

IN DIESEM ABSCHNITT

EINSTELLUNGEN FÜR MELDUNGEN

Bei der Arbeit von Kaspersky Rescue Disk treten unterschiedliche Ereignisse ein. Sie können informativen Charakter besitzen oder wichtige Informationen enthalten. Ein Ereignis kann beispielsweise über die erfolgreiche Aktualisierung des Programms informieren oder einen Fehler betreffen, der dringend behoben werden muss.

Bei der Arbeit sendet Kaspersky Rescue Disk Meldungen der folgenden Typen:

- **Kritische Meldungen –** Meldungen über Ereignisse mit kritischer Priorität, die auf Probleme bei der Arbeit von Kaspersky Rescue Disk oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Beispiele: beschädigte Programm-Datenbanken oder abgelaufener Schlüssel.
- **Störungen bei der Programmarbeit** – Meldungen über Ereignisse, die zur Funktionsunfähigkeit der Anwendung führen. Beispiele: fehlender Schlüssel oder fehlende Programm-Datenbanken.
- **Wichtige Meldungen –** Meldungen über Ereignisse, die unbedingt beachtet werden sollten, weil Sie wichtige Situationen bei der Arbeit von Kaspersky Rescue Disk betreffen. Beispiele: Schutz wurde deaktiviert oder Computer wurde lange nicht auf Viren untersucht.
- **Sonstige Meldungen** – Meldungen über Ereignisse mit informativem Charakter, die in der Regel keine wichtigen Informationen enthalten. Beispiele: Alle gefährlichen Objekte wurden neutralisiert.

Um die Ereignisbenachrichtigungen zu aktivieren / zu deaktivieren, klicken Sie im oberen Bereich des Programmhauptfensters auf **Einstellungen**, wählen Sie den Abschnitt **Meldungen** und aktivieren Sie das Kontrollkästchen **Ereignisse melden**.

Um sich über die Ereignisse bei der Arbeit von Kaspersky Rescue Disk informieren zu lassen, können Sie den Dienst für Benachrichtigungen verwenden. In der Grundeinstellung erfolgen die Meldungen für alle Ereignisse durch Popupmeldungen. Außerdem können Sie das Senden von Meldungen deaktivieren (siehe Abschnitt "Benachrichtigungen deaktivieren" auf S. 60) und bestimmen, über welche Ereignisse Sie informiert werden möchten.

SIEHE AUCH

ANPASSEN VON BENACHRICHTIGUNGEN

Gehen Sie folgendermaßen vor, um die Parameter für Benachrichtigungen anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Fensterseite den Abschnitt **Meldungen**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Meldungen** die Kontrollkästchen für die Ereignisse, über die eine Meldung erfolgen soll.

SIEHE AUCH

Einstellungen für Meldungen 59

BENACHRICHTIGUNGEN DEAKTIVIEREN

Gehen Sie folgendermaßen vor, um das Senden von Meldungen zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Fensterseite den Abschnitt **Meldungen**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Ereignisse melden**.

Informationen über Ereignisse, die bei der Arbeit des Programms eintreten, werden auch dann im Bericht über die Arbeit von Kaspersky Rescue Disk protokolliert, wenn das Senden von Meldungen deaktiviert wurde.

SIEHE AUCH

Einstellungen für Meldungen 59

BERICHTE UND SPEICHER

Der Abschnitt enthält Informationen über die Parameter, welche die Arbeit mit den Dateien von Berichten und Speichern von Kaspersky Rescue Disk regeln.

IN DIESEM ABSCHNITT

EINSTELLUNGEN FÜR BERICHTE UND SPEICHER

Der Abschnitt enthält Informationen über die Parameter, welche die Arbeit mit den Datendateien von Kaspersky Rescue Disk regeln.

Zur Datenverwaltung des Programms gehören Objekte, die bei der Arbeit von Kaspersky Rescue Disk in die Quarantäne (siehe Abschnitt "Quarantäne" auf S. 33) oder ins Backup (siehe Abschnitt "Backup" auf S. 34). Außerdem zählen dazu die Berichtsdateien über die Aufgabenausführung (siehe Abschnitt "Berichte" auf S. 36).

Im Abschnitt **Berichte und Speicher** des Konfigurationsfensters von Kaspersky Rescue Disk können Sie:

- Einträge zum Bericht hinzufügen (siehe Abschnitt "Aufnahme unkritischer Ereignisse in den Bericht" auf S. 62).

  Sie können festlegen, dass dem Schutzbericht auch Einträge über unkritische Ereignisse hinzugefügt werden. In der Grundeinstellung werden diese Einträge nicht aufgezeichnet.

- Einstellungen für das Speichern von Berichten ändern (siehe Abschnitt "Berichte speichern" auf S. 62).

  Sie können die maximale Speicherdauer für Berichte und die maximale Größe von Berichtsdateien angeben. Außerdem können Sie die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

- Informationen aus Berichten löschen (siehe Abschnitt "Berichte leeren" auf S. 63).

  Informationen über die Arbeit von Kaspersky Rescue Disk werden in den Berichten aufgezeichnet. Diese können bereinigt werden.

- Einstellungen für das Speichern von Quarantäne- und Backup-Objekten ändern (siehe Abschnitt "Quarantäne- und Backup-Objekte speichern" auf S. 63).

  Sie können eine maximale Speicherdauer für Objekte in der Quarantäne und Sicherungskopien im Backup festlegen (Kontrollkästchen ☑ **Objekte speichern für maximal**). Standardmäßig beträgt die Speicherdauer für Quarantäneobjekte 30 Tage. Danach werden die Objekte gelöscht. Sie können die maximale Speicherdauer ändern oder diese Beschränkung völlig aufheben. Außerdem kann die Größe des Datenspeichers beschränkt werden (Kontrollkästchen ☑ **Maximale Größe**). Die maximale Größe beträgt standardmäßig 100 MB. Sie können die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

SIEHE AUCH

AUFNAHME UNKRITISCHER EREIGNISSE IN DEN BERICHT

Um unkritische Ereignisse in den Bericht aufzunehmen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Berichte und Speicher** aus.
3. Aktivieren Sie im rechten Teil des Fensters im Block **Berichte** das Kontrollkästchen **Nicht kritische Ereignisse protokollieren**.

SIEHE AUCH

BERICHTE SPEICHERN

Gehen Sie folgendermaßen vor, um die Parameter für das Speichern von Berichten anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Berichte und Speicher** aus.

3. Legen Sie auf der rechten Fensterseite im Block **Berichte** Folgendes fest:

   - Die maximale Speicherdauer für Ereignisberichte (Kontrollkästchen ☑ **Berichte speichern für maximal**). Standardmäßig beträgt dieser Wert 30 Tage. Danach werden die Objekte gelöscht. Die maximale Speicherdauer kann geändert oder völlig aufgehoben werden.

   - Die maximale Größe einer Berichtsdatei (Kontrollkästchen ☑ **Maximale Dateigröße**). Die maximale Größe beträgt standardmäßig 1024 MB. Wenn die maximale Größe erreicht wird, wird der Inhalt der Datei mit neuen Einträgen ersetzt. Sie können die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

SIEHE AUCH

Einstellungen für Berichte und Speicher 61

BERICHTE LÖSCHEN

➡ *Um die* Berichte *zu leeren, gehen Sie folgendermaßen vor*:

1. Öffnen Sie das Programmhauptfenster.

2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Berichte und Speicher** aus.

3. Klicken Sie auf der rechten Fensterseite im Block **Berichte** auf **Leeren**.

4. Aktivieren Sie im Fenster **Informationen aus Berichten löschen** die Kontrollkästchen für die Berichtskategorien, die Sie bereinigen möchten.

SIEHE AUCH

Einstellungen für Berichte und Speicher 61

QUARANTÄNE- UND BACKUP-OBJEKTE SPEICHERN

➡ *Gehen Sie folgendermaßen vor, um die Parameter für das Speichern von Quarantäne- und Backup-Objekten anzupassen:*

1. Öffnen Sie das Programmhauptfenster.

2. Verwenden Sie im oberen Bereich des Fensters den Link **Einstellungen**. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Berichte und Speicher** aus.

3. Aktivieren Sie auf der rechten Fensterseite im Block **Quarantäne und Backup** die erforderlichen Kontrollkästchen:

   - **Objekte speichern für maximal** – gibt den Zeitraum an, über den die Objekte in der Quarantäne und im Backup gespeichert bleiben.
   - **Maximale Größe** – gibt die maximale Größe des Datenspeichers an.

   Nach Ablauf des festgelegten Zeitraums und bei voller Ausnutzung des maximalen Speichervolumens werden die am längsten in der Quarantäne oder im Backup befindlichen Objekte entfernt.

SIEHE AUCH

Quarantäne und Backup 33

Einstellungen für Berichte und Speicher 61

ARBEIT VON KASPERSKY RESCUE DISK BEENDEN

Gehen Sie folgendermaßen vor, um Kaspersky Rescue Disk zu beenden:

1. Klicken Sie auf das Symbol auf der Taskleiste in der linken unteren Ecke des Bildschirms. Das Systemmenü wird geöffnet.
2. Wählen Sie im erscheinenden Menü den Punkt **Computer ausschalten** aus.

   Es erscheint ein Dialogfenster mit der Frage **Möchten Sie den Computer wirklich ausschalten?**
3. Klicken Sie auf die Schaltfläche **Ja**.

ARBEIT MIT KASPERSKY RESCUE DISK IM TEXTMODUS

Dieser Abschnitt beschreibt die Arbeit mit Kaspersky Rescue Disk im Textmodus.

IN DIESEM ABSCHNITT

ÜBER DEN TEXTMODUS

Beim Textmodus handelt es sich um eine Benutzeroberfläche, die zur Ein- und Ausgabe sowie zur Darstellung von Informationen ausschließlich alphanumerische Zeichen und Pseudografik verwendet. Der Textmodus zeichnet sich durch geringe Anforderungen an die Ressourcen der Ein-/Ausgabehardware (insbesondere an den Speicher) und eine schnelle Darstellung der Informationen aus.

Der Textmodus von Kaspersky Rescue Disk vereint eine Befehlszeilenoberfläche mit dem Konsolenmodus, der vom Dateimanager Midnight Commander bereitgestellt wird.

Im Textmodus sind folgende Funktionen verfügbar:

- Netzwerk konfigurieren (Netzwerkadapter, Proxyserver);
- Start der Konsole von Kaspersky Rescue Disk;
- Untersuchung von Objekten (Autostart-Objekte, Bootsektoren, Laufwerke, Verzeichnisse auf Laufwerken, aller Objekte);
- Datenbank-Update;
- Rollback zum vorherigen Update;
- Hilfe zur Befehlssyntax;
- Computerneustart;
- Beenden von Kaspersky Rescue Disk und Herunterfahren des Computers.

Im Textmodus können Sie lediglich Aufgaben zur Untersuchung von Objekten und zum Update starten. Zur Änderung der Aufgabenparameter muss das Programm im Grafikmodus gestartet werden (siehe Abschnitt "Arbeit mit Kaspersky Rescue Disk im Grafikmodus" auf S. 19).

ARBEIT MIT DEM DATEIMANAGER

Dieser Abschnitt beschreibt die Funktionen, die für den Datei Manager von Kaspersky Rescue Disk im Textmodus verfügbar sind.

IN DIESEM ABSCHNITT

NETZWERK KONFIGURIEREN

Um den Netzwerkadapter anzupassen und die Proxyserver-Einstellungen zu ändern, gehen Sie folgendermaßen vor:

1. Im Benutzermenü wählen Sie den Punkt **Netzwerk konfigurieren**. Das Fenster **Konfiguration des Netzwerkadapters** wird geöffnet.
2. Wählen Sie im folgenden Fenster eine der folgenden Optionen:
   - **Netzwerkadapter konfigurieren** – um die Parameter für den Netzwerkadapter festlegen.

     Wählen Sie den Netzwerkadapter, dessen Parameter Sie ändern möchten. Klicken Sie auf die Schaltfläche **OK**. Das Konfigurationsfenster des gewählten Netzwerkadapters wird geöffnet. Um seine Parameter zu ändern, klicken Sie auf die Schaltfläche **Ja**. Wählen Sie im folgenden Fenster eine der folgenden Varianten:
     - **DHCP** – Netzwerkadapter automatisch anpassen.
     - **Manuell einrichten** – Parameter des Netzwerkadapters manuell festlegen. Klicken Sie auf die Schaltfläche **OK**. Legen Sie im folgenden Fenster die Parameter für den Netzwerkadapter fest.

     Klicken Sie nach erfolgreichem Abschluss der Konfiguration des Netzwerkadapters auf **OK**.
   - **Proxyserver konfigurieren** – um die Proxyserver-Einstellungen angeben.

     Klicken Sie auf die Schaltfläche **OK**. Geben Sie im folgenden Fenster die Parameter für den Proxyserver an. Klicken Sie auf die Schaltfläche **OK**.

START DER KONSOLE VON KASPERSKY RESCUE DISK

Um die Konsole von Kaspersky Rescue Disk zu starten,

wählen Sie im Benutzermenü den gleichnamigen Punkt aus.

VIRENSUCHE

➧ *Um die Untersuchung der Objekte zu starten,*

wählen Sie im Benutzermenü einen der folgenden Punkte aus:

- **<Laufwerk> untersuchen** – Kaspersky Rescue Disk untersucht alle Objekte (Dateien) auf dem Laufwerk auf Viren. Wird das Objekt als infiziert oder verdächtig eingestuft, wird dem Benutzer vorgeschlagen, bestimmte Aktionen mit diesem Objekt auszuführen.

  Nach entsprechender Bearbeitung des infizierten / verdächtigen Objekts entfernt Kaspersky Rescue Disk den Verweis auf dieses Objekt aus der Registry und die Dateien der Systemordner von Windows.

- **Alle Objekte untersuchen** – Kaspersky Rescue Disk untersucht alle Dateien aller Laufwerke, einschließlich der Autostart-Objekte und der Bootsektoren.

- **Autostart-Objekte untersuchen** – Kaspersky Rescue Disk untersucht die Registrierung sowie Dateien mit den Erweiterungen inf, ini, bat der Dienstkataloge von Windows auf allen verbundenen Laufwerken. Jedes Objekt wird auf Viren untersucht. Wird das Objekt als infiziert oder verdächtig eingestuft, wird dem Benutzer vorgeschlagen, bestimmte Aktionen mit diesem Objekt auszuführen.

  Nach entsprechender Bearbeitung des infizierten / verdächtigen Objekts entfernt Kaspersky Rescue Disk den Verweis auf dieses Objekt aus der Registry und die Dateien der Systemordner von Windows.

- **Laufwerksbootsektoren untersuchen** – Kaspersky Rescue Disk untersucht jeden Bootsektor des Laufwerks auf Schadobjekte. Wird ein Schadobjekt gefunden, wird dem Benutzer vorgeschlagen, bestimmte Aktionen mit diesem Objekt auszuführen.

  Nach entsprechender Bearbeitung des Schadobjekts entfernt Kaspersky Rescue Disk den Verweis auf dieses Objekt aus der Registry und die Dateien der Systemordner von Windows.

UPDATE VON KASPERSKY RESCUE DISK

➧ *Um die Updateaufgabe zu starten,*

wählen Sie im Benutzermenü den Punkt **Update ausführen**.

ROLLBACK ZU DEN VORHERIGEN DATENBANKEN

➧ *Um zu den vorherigen Datenbanken zurückzukehren,*

wählen Sie im Benutzermenü den gleichnamigen Punkt aus.

ANZEIGEN DER HILFE

➧ *Zur Anzeige der Shortcuts für den Dateimanager*

wählen Sie im Benutzermenü den Punkt **Hilfe**.

ARBEIT VON KASPERSKY RESCUE DISK BEENDEN

➧ *Gehen Sie folgendermaßen vor, um Kaspersky Rescue Disk zu starten,*

wählen Sie im Benutzermenü oder im Befehlsverzeichnis den Punkt **Computer ausschalten** / **Computer neu starten** aus.

ARBEIT AUS DER BEFEHLSZEILE

Dieser Abschnitt beschreibt das Arbeiten in der Befehlszeile von Kaspersky Rescue Disk im Textmodus.

IN DIESEM ABSCHNITT

SYNTAX DER BEFEHLSZEILE

Syntax der Befehlszeile:

```
<Befehl> [Parameter]
```

Als Befehl werden verwendet:

HELP	Hilfe über die Befehlssyntax, Anzeige einer Befehlsliste
SCAN	Untersuchung von Objekten auf das Vorhandensein von Viren
UPDATE	Updateaufgabe starten
ROLLBACK	Rollback zum vorherigen Update
EXIT	Arbeit von Kaspersky Rescue Disk beenden

VIRENSUCHE

Die Befehlszeile zum Starten der Virenuntersuchung eines bestimmten Bereichs und zur Verarbeitung von schädlichen Objekten besitzt generell folgendes Aussehen:

```
SCAN [<Untersuchungsobjekt>] [<Aktion>] [<Dateitypen>] [<Ausnahmen>]
[<Berichtsparameter>]
```

Laufwerksbezeichnungen müssen nur in Großbuchstaben eingegeben werden. Beispiel: C:/file.txt, wobei C die Bezeichnung des Laufwerks ist.

Beschreibung der Parameter:

<Untersuchungsobjekt> – Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
<files>	Liste mit den Pfaden der Dateien und / /oder Ordner für die Untersuchung. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen. Kommentare: • Wenn der Objektname ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt. • Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.
<disc_name>:/<folder>	Einen bestimmten Ordner untersuchen, wobei <disc_name> – Name des Laufwerks, und <folder> – Pfad des zu untersuchenden Ordners.
<Aktion> – Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert **-i8** entspricht.	
-i0	Keine Aktion ausführen, sondern Informationen im Bericht protokollieren.
-i1	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen.
-i2	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; infizierte Objekte aus Containern (zusammengesetzten Objekten) nicht löschen; Container mit ausführbarer Kopfzeile (sfx-Archive) löschen.
-i3	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
-i4	Infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
-i8	Beim Fund eines infizierten Objekts den Benutzer nach der Aktion fragen.
-i9	Den Benutzer nach der Aktion fragen, wenn die Untersuchung abgeschlossen wird.

<Dateitypen> – Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht.	
-fe	Nur infizierbare Dateien nach Erweiterung untersuchen
-fi	Nur infizierbare Dateien nach Inhalt untersuchen
-fa	Alle Dateien untersuchen
<Ausnahmen> – Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
-e:a	Archive nicht untersuchen
-e:b	Mail-Datenbanken nicht untersuchen.
-e:m	E-Mail-Nachrichten im Format plain text nicht untersuchen
-e:<filemask>	Objekte nach Maske nicht untersuchen
-e:<Sekunden>	Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter **<Sekunden>** angegebene Zeitraum.
-es:<Container size limit>	Zusammengesetzte Dateien überspringen, deren Größe (in MB) über dem Wert liegt, der durch den Parameter **<Container size limit>** angegeben wird.

Beispiel:

➡ *Untersuchung des Verzeichnisses Dokumente und Einstellungen und des Laufwerks <D> starten:*

```
SCAN D: "C:/Dokumente und Einstellungen"
```

UPDATE VON KASPERSKY RESCUE DISK

Der Befehl für das Update der Datenbanken und Programm-Module von Kaspersky Rescue Disk besitzt folgende Syntax:

```
UPDATE [<Updatequelle>] [-R[A]:<Berichtsdatei>]
```

Laufwerksbezeichnungen müssen nur in Großbuchstaben eingegeben werden. Beispiel: C:/file.txt, wobei C die Bezeichnung des Laufwerks ist.

Beschreibung der Parameter:

<Updatequelle>	HTTP-, FTP-Server oder Netzwerkordner für den Download von Updates. Als Wert für diesen Parameter kann der vollständige Pfad oder die URL-Adresse der Updatequelle angegeben werden. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Parametern des Diensts für das Update von Kaspersky Rescue Disk übernommen.
-R[A]:<Berichtsdatei>	**-R:<Berichtsdatei>** – nur wichtige Ereignisse im Bericht protokollieren. **-RA:<Berichtsdatei>** – alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Beispiel:

➡ *Update der Datenbanken, alle Ereignisse im Bericht protokollieren:*

```
UPDATE -RA:C:/avbases_upd.txt
```

ROLLBACK ZUM VORHERIGEN UPDATE

Befehlssyntax:

```
ROLLBACK [-R[A]:<Berichtsdatei>]
```

Laufwerksbezeichnungen müssen nur in Großbuchstaben eingegeben werden. Beispiel: C:/file.txt, wobei C die Bezeichnung des Laufwerks ist.

Beschreibung der Parameter:

-R[A]:<Berichtsdatei>	**-R:<Berichtsdatei>** – nur wichtige Ereignisse im Bericht protokollieren. **/RA:<Berichtsdatei>** – alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Beispiel:

➡ *Rollback des Berichts:*

```
ROLLBACK -RA:C:/rollback.txt
```

ANZEIGEN DER HILFE

Zur Anzeige der Hilfe über die Syntax der Befehlszeile dient folgender Befehl:

```
HELP
```

Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
<Befehl> -?
HELP <Befehl>
```

ARBEIT VON KASPERSKY RESCUE DISK BEENDEN

Um die Arbeit mit Kaspersky Rescue Disk über die Befehlszeilensyntax zu beenden, dient folgender Befehl:

```
exit
```

HARDWAREINFORMATIONEN

Die Aufgabe **Hardwareinformationen** kann verwendet werden, wenn aufgrund mangelnder Hardwareunterstützung ein Start von Kaspersky Rescue Disk weder im grafischen Modus noch im Textmodus möglich ist.

Die Aufgabe **Hardwareinformationen** ermöglicht die Speicherung der Informationen über die Systemhardware in elektronischer Form. Schließen Sie vor dem Start der Aufgabe den Wechseldatenträger an, auf dem die Hardwareinformationen gespeichert werden sollen.

Die Hardwareinformationen können nicht auf einem auswechselbaren CD / DVD-RW-Laufwerk gespeichert werden.

Im Anschluss an die Aufgabe stehen in dem sich öffnenden Dialogfenster die Optionen zur Speicherung der Informationen sowie zum Neustart oder zum Herunterfahren des Computers zur Auswahl. Zur Navigation zwischen den Optionen, betätigen Sie die Taste **TAB**. Um Ihre Auswahl zu bestätigen, betätigen Sie die Taste **ENTER**.

Speichern Sie die durch diese Funktion bereitgestellten Informationen auf ihrem Wechseldatenträger und senden Sie diese an die Spezialisten des Technischen Supports (siehe Abschnitt "Kontaktaufnahme mit dem Technischen Support" auf S. 74).

Falls Ihnen kein Wechseldatenträger zur Verfügung steht, können Sie die Informationen handschriftlich notieren oder vom Bildschirm abfotografieren.

EINSCHRÄNKUNGEN BEI DER PROGRAMMARBEIT

Momentan liegen folgende Beschränkungen bei der Arbeit des Programms vor:

- Bei Auswahl des Grafikmodus fährt der Computer herunter, ohne Kaspersky Rescue Disk zu laden. Der wahrscheinlichste Grund - Probleme beim Herunterladen des grafischen Subsystems, der Treiber für den Videoadapter oder für ein Eingabegerät wird nicht gefunden.

- Kaspersky Rescue Disk zeigt keine logischen Laufwerke während der Auswahl eines Untersuchungsbereichs an. Es werden nur Bootsektoren angezeigt. Der wahrscheinlichste Grund – Dateisysteme auf den angeschlossenen Festplatten und USB-Geräten wurden, möglicherweise wegen der RAID-Verwendung, nicht ermittelt.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Wenn bei der Verwendung von Kaspersky Rescue Disk Probleme auftreten sollten, prüfen Sie zuerst, ob die Dokumentation, die Hilfe, die Wissensdatenbank auf der Seite des Technischen Supports von Kaspersky Lab oder das Benutzerforum keine Lösung dafür bieten.

Wenn Sie keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky Lab. Dies ist auf folgende Weise möglich:

- aus Mein Kaspersky Account eine Anfrage an die Webseite des Technischen Supports senden;
- telefonisch.

Die Spezialisten des Technischen Supports beantworten Ihre Fragen zur Installation, Aktivierung und Verwendung des Programms. Wenn Ihr Computer infiziert wurde, helfen sie Ihnen dabei, die Folgen der schädlichen Malware-Aktionen zu beheben.

Bitte beachten Sie die Support-Richtlinien, bevor Sie sich an den Technischen Support wenden.

Wenn Sie sich an den Technischen Support wenden, bitten die Support-Experten Sie möglicherweise darum, eine Protokolldatei zu erstellen und diese an den Technischen Support zu senden.

IN DIESEM ABSCHNITT

MEIN KASPERSKY ACCOUNT

Mein Kaspersky Account ist Ihr persönlicher Bereich auf der Seite des Technischen Supports. Dort können Sie folgende Aktionen ausführen:

- Anfragen an den Technischen Support und an das Virenlabor senden;
- ohne E-Mail mit dem Technischen Support kommunizieren;
- Status Ihrer Anfragen in Echtzeit verfolgen;
- Verlauf Ihrer Zugriffe auf den Technischen Support ansehen.

Um auf die Seite zum Einloggen in Mein Kaspersky Account zu gelangen, geben Sie in der Adressleiste des Browsers folgende Adresse ein https://my.kaspersky.de.

Wenn Sie noch keinen Kaspersky Account besitzen, können Sie sich auf der Registrierungsseite anmelden. Geben Sie hier Ihre E-Mail-Adresse und ein Kennwort für den Zugriff auf Ihren Kaspersky Account an.

Beachten Sie, dass bestimmte Anfragen nicht an den Technischen Support, sondern an das Virenlabor gerichtet werden müssen. Dazu zählen folgende Arten von Anfragen:

- Unbekanntes Schadprogramm – Sie haben den Verdacht, dass ein bestimmtes Objekt schädlich ist, obwohl Kaspersky Rescue Disk es nicht als Malware einstuft.
- Viren-Fehlalarm – Kaspersky Rescue Disk stuft eine bestimmte Datei als infiziert ein, während Sie sicher sind, dass die Datei virenfrei ist.
- Anfrage für eine Beschreibung eines Schadprogramms – Sie möchten die Beschreibung eines bestimmten Virus erhalten.

Anfragen an das Virenlabor sind ohne Anmeldung bei Mein Kaspersky Account auf der Seite mit dem Anfrageformular möglich.

Weitere Informationen finden Sie auf der Seite des Technischen Supports unter den FAQs zu Mein Kaspersky Account.

TECHNISCHER SUPPORT AM TELEFON

Zur Lösung dringender Probleme können Sie jederzeit Ihren lokalen Technischen Support anrufen. Wenn Sie sich an den russischsprachigen oder internationalen Technischen Support wenden, um Hilfe zu erhalten, vergessen Sie bitte nicht, die dafür erforderlichen Informationen über Ihren Computer und das installierte Antiviren-Programm bereitzuhalten. Dadurch können unsere Spezialisten Ihnen möglichst schnell helfen.

ERSTELLUNG UND SPEICHERUNG EINER PROTOKOLLDATEI

Wenn Störungen von Kaspersky Rescue Disk auftreten, können die Fachleute des Technischen Supports von Kaspersky Lab Sie darum bitten, eine Protokolldatei zu erstellen.

Gehen Sie folgendermaßen vor, um eine Protokolldatei zu erstellen und zu speichern:

1. Wählen Sie im Bootmanager mit Hilfe der Cursortasten die Sprache der Grafikoberfläche aus. Klicken Sie auf die Taste **ENTER**.

   Es erscheint ein Fenster mit den zur Verfügung stehenden Optionen.

2. Wählen Sie den gewünschten Bootmodus aus.
3. Drücken Sie die Taste **E**.
4. Geben Sie am Ende der ersten Zeile nach dem Wort **quiet** ein Leerzeichen und das Wort **trace** ein.
5. Drücken Sie die Tastenkombination **STRG+X**.

   Die Protokolldatei wird gespeichert.

   Während der Arbeit mit Kaspersky Rescue Disk haben Sie über den Task-Manager Zugriff auf die Datei. Die Datei wird unter **/discs/<Festplatte>:/Kaspersky Rescue Disk/avp<individuelle Kombination aus Datum, Uhrzeit und internen Daten>.log** abgelegt.

   Nach Abschluss der Arbeit mit Kaspersky Rescue Disk wird die Datei als Archiv gespeichert und unter **<Festplatte>:/Kaspersky Rescue Disk/kavrescue_sysinfo_<Speicherdatum der Datei>** abgelegt.

GLOSSAR

A

AUSNAHME

Eine Ausnahme ist ein Objekt, das von der Untersuchung durch das Kaspersky-Lab-Programm ausgeschlossen wird. Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden. Für jede Aufgabe können individuelle Ausnahmen festgelegt werden.

B

BACKUP

Spezieller Speicher für Sicherungskopien von Objekten, die vor einer Desinfektion oder vor dem Löschen angelegt werden.

D

DATENBANK-UPDATE

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Datenbanken von den Kaspersky-Lab-Updateservern auf den Computer kopiert und automatisch von der Anwendung übernommen.

DATENBANKEN

Datenbanken, die von den Kaspersky-Lab-Spezialisten gepflegt werden und eine genaue Beschreibung aller momentan existierenden Bedrohungen der Computersicherheit sowie Methoden zu ihrer Identifikation und Desinfektion enthalten. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen. Um die Erkennungsqualität für Bedrohungen zu steigern, empfehlen wir, regelmäßig Updates für die Datenbanken von den Kaspersky-Lab-Updateservern herunterzuladen.

DESINFEKTION VON OBJEKTEN

Methode zur Bearbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder eine Entscheidung darüber getroffen wird, dass die Desinfektion von Objekten nicht möglich ist. Die Desinfektion von Objekten erfolgt auf Basis der Einträge in den Datenbänken. Wenn die Desinfektion als primäre Aktion für ein Objekt gilt (erste Aktion mit dem Objekt, die sofort nach seinem Fund ausgeführt wird), wird eine Sicherungskopie des Objekts angelegt, bevor die Desinfektion ausgeführt wird. Bei der Desinfektion können Daten teilweise verloren gehen. Sie können diese Kopie verwenden, um ein Objekt in dem Zustand wiederherzustellen, wie vor der Desinfektion.

E

EMPFOHLENE STUFE

Sicherheitsstufe, deren Funktionsparameter von Kaspersky Lab empfohlen werden und die einen optimalen Schutz Ihres Computers gewährleistet. Diese Stufe wird in der Grundeinstellung verwendet.

H

HEURISTISCHE ANALYSE

Technologie zum Erkennen von Bedrohungen, die sich nicht mit Hilfe der Datenbanken von Anti-Virus identifizieren lassen. Es wird erlaubt, Objekte zu finden, die verdächtig sind, durch einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus infizierte zu sein.

Mit Hilfe der heuristischen Analyse werden bis zu 92 % der neuen Bedrohungen erkannt. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Dateien, die mit Hilfe der heuristischen Analyse gefunden werden, nennt man verdächtig.

I

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Untersuchung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten, weil dies zur Infektion Ihres Computers führen kann.

K

KASPERSKY-LAB-UPDATESERVER

Liste der HTTP- und FTP-Server von Kaspersky Lab, von denen das Programm die Updates für Datenbanken und Module auf Ihren Computer herunterlädt.

L

LAUFWERKSBOOTSEKTOR

Ein Bootsektor ist ein spezieller Sektor auf der Festplatte eines Computers, auf einer Diskette oder auf einem anderen Gerät zur Datenspeicherung. Er enthält Angaben über das Dateisystem des Datenträgers und ein Bootprogramm, das für den Start des Betriebssystems verantwortlich ist.

Laufwerksbootsektoren können von so genannten Bootviren infiziert werden. Die Kaspersky-Lab-Anwendung erlaubt es, Bootsektoren auf Viren zu untersuchen und infizierte Sektoren zu desinfizieren.

M

MÖGLICHERWEISE INFIZIERTES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Infizierte Dateien können mit Hilfe der heuristischen Analyse gefunden werden.

O

OBJEKT LÖSCHEN

Methode zur Objektbearbeitung, bei der das Objekt physikalisch von dem Ort gelöscht wird, an dem es vom Programm gefunden wurde (Festplatte, Ordner, Netzwerkressource). Diese Bearbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion aus bestimmten Gründen nicht möglich ist.

OBJEKTE IN DIE QUARANTÄNE VERSCHIEBEN

Verarbeitungsmethode für ein möglicherweise infiziertes Objekt. Dabei wird der Zugriff auf das Objekt gesperrt und das Objekt wird vom ursprünglichen Speicherort in den Quarantäneordner verschoben. Dort wird es in verschlüsselter Form gespeichert, um eine Infektion auszuschließen.

P

PROGRAMMEINSTELLUNGEN

Einstellungen für die Arbeit des Programms, die für alle Aufgabentypen gleich sind und sich auf das gesamte Programm beziehen (z.B. Leistungseinstellungen für das Programm, Einstellungen für das Berichtswesen, Backup-Einstellungen).

PROXYSERVER

Dienst in Computernetzwerken, mit dem Clients indirekte Anfragen an andere Netzwerkdienste richten können. Zunächst baut der Client eine Verbindung zu einem Proxyserver auf und fragt nach einer bestimmten Ressource (zum Beispiel nach einer Datei), die auf einem anderen Server liegt. Dann stellt der Proxyserver mit dem angegebenen Server eine Verbindung her und nimmt von ihm die Ressource entgegen oder schreibt die Ressource in seinen eigenen Cache (falls der Proxy einen Cache besitzt). In einigen Fällen kann die Client-Anfrage oder Server-Antwort vom Proxyserver zu bestimmten Zwecken geändert werden.

Q

QUARANTÄNE

Ein bestimmter Ordner, in den alle möglicherweise infizierten Objekte verschoben werden, die bei der Untersuchung oder im Rahmen des Echtzeitschutzes gefunden werden.

S

SCHUTZSTATUS

Aktueller Schutzstatus, der das Sicherheitsniveau des Computers charakterisiert.

U

UPDATE

Vorgang, bei dem vorhandene Dateien (Datenbanken oder Programm-Module) durch neue Dateien ersetzt bzw. neue Dateien hinzugefügt werden. Die neuen Dateien werden von den Kaspersky-Lab-Updateservern heruntergeladen.

W

WIEDERHERSTELLUNG

Ein Originalobjekt wird aus der Quarantäne oder aus dem Backup entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

KASPERSKY LAB ZAO

Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an: Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Die Zentrale befindet sich in Russland, es gibt Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Benelux-Ländern, China, Polen, Rumänien und in den USA (Kalifornien). In Frankreich wurde eine neue Tochtergesellschaft gegründet, das Europäische Zentrum für Antiviren-Forschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das sind heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome und sechzehn einen Doktortitel besitzen. Die führenden Virusanalytiker von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens sind das einzigartige Wissen und die Erfahren, die die Mitarbeiter im Laufe des mehr als vierzehnjährigen ununterbrochenen Kampfes gegen Viren gesammelt haben. Dank der ständigen Analyse von Virenaktivitäten können wir Tendenzen bei der Malware-Entwicklung vorhersagen und frühzeitig Benutzern einen zuverlässigen Schutz vor neuen Angriffen an die Hand geben. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab. Wir sind unseren Wettbewerbern stets einen Schritt voraus und bieten unseren Kunden den besten Schutz.

Aufgrund der jahrelangen Tätigkeit wurde das Unternehmen zum führenden Entwickler von Technologien zum Schutz vor Viren. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus® und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Bequeme Steuerelemente versetzen die Benutzer in die Lage, den Antivirenschutz von Computern und Unternehmensnetzwerken maximal zu automatisieren. Viele internationale Developer verwendeten in ihrer Software den Kernel von Kaspersky Anti-Virus, beispielsweise: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir projektieren, realisieren und begleiten Antiviren-Komplex-Lösungen von Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Wir haben für unsere Benutzer einen technischen Kundendienst in mehreren Sprachen eingerichtet.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir beraten Sie gern detailliert über das Telefon oder E-Mail. Auf Ihre Fragen bekommen Sie eine vollständige und erschöpfende Antwort.

Webseite von Kaspersky Lab:	http://www.kaspersky.de
Viren-Enzyklopädie:	http://www.viruslist.com/de
Antiviren-Labor:	newvirus@kaspersky.com (nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de (für Fragen an die Virenanalytiker)
Webforum von Kaspersky Lab:	http://forum.kaspersky.com

INFORMATION ÜBER FREMDCODE

Für die Erstellung des Programms wurde Code von Drittanbietern verwendet.

IN DIESEM ABSCHNITT

PROGRAMMCODE

Informationen über den Programmcode von Drittanbietern, der bei der Erstellung des Programms verwendet wurde, befinden sich in der Datei rescue/help/License_notice_1.txt.

ENTWICKLERTOOLS

Informationen über Entwicklertools, Utilities und sonstige Komponenten von Drittanbietern, die bei der Erstellung des Programms verwendet wurden, befinden sich in der Datei /rescue/help/License_notice_2.txt.

ENTHALTENER PROGRAMMCODE

Das Programm enthält integrierten unabhängigen Programmcode von Drittanbietern in binärer Form. Der Lizenztext für Code, der auf Grundlage der Lizenzen GNU GPL und GNU LGPL verwendet wird, ist in der Datei /rescue/help/License_notice_3.txt enthalten.

SONSTIGE INFORMATIONEN

Für die Überprüfung elektronischer digitaler Signaturen wird die Krypto-Bibliothek (Programmbibliothek zum Informationsschutz - PBSI) "Agave-S" verwendet, die von der OOO "R-Alpha" entwickelt wurde.

Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software"). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert.

Zusätzliche Informationen über Fremdcode befinden sich in der Datei /rescue/help/License_notice_4.txt.

SACHREGISTER

A

B

D

G

H

I

K

M

N

P

Q

S

T

U

V